BEC 7800N

802.11n Dual WAN
ADSL2+ Firewall Router

User Manual

Version released 1.02.dr7

Last revised date 5-12-2008

Table of Contents

Chapter 1: Introduction 1
Introduction to your Router 1
Features 2
Chapter 2: Installing the Router 4
Important note for using this router 4
Package Contents 5
Device Description 6
The Front LEDs 6
The Rear Ports 7
Cabling 8
Chapter 3: Basic Installation 9
Connecting Your Router 10
Network Configuration 11
Factory Default Settings 17
Information from your ISP 18
Chapter 4: Configuration 19
Quick Start 20
Status (Basic Mode) 31
Cofiguration (Basic Mode) 32
WAN – Main Port (ADSL) 32
WAN – Main Port (EWAN) 37
WLAN 39
Status (Advanced Mode) 43
ADSL 44
ARP 45
DHCP 45
System Log 46

Configuration (Advanced Mode) 47
LAN 47
Ethernet 47
IP Alias 47
Wireless 48
Wireless Security 51
DHCP Server 53
WAN 54
WAN Profile (ADSL) 54
WAN Profile – Main Port (EWAN) 60
ADSL Mode 64
System 65
Time Zone 65
Firmware Upgrade 66
Backup / Restore 67
Restart 68
User Management 68
Firewall 69
Packet Filter 69
MAC Filter 71
Block WAN Ping 71
Virtual Server 72
Port Mapping 73
DMZ 74
Advanced 75
Static Route 75
Dynamic DNS 75
VLAN 76
Device Management 77
IGMP 85

TR-069 Client 85
Remote Access 86
Appendix: Product Support & Contact 87

Chapter 1: Introduction

Introduction to your Router

Thank you for purchasing BEC 7800N Router. Your new router is an all-in-one unit that combines an ADSL modem, ADSL2/2+ router and Ethernet network switch to provide everything you need to get the machines on your network connected to the Internet over an ADSL broadband connection.

BEC 7800N router complies with ADSL2+ standards for deployment worldwide and supports downstream rates of up to 24 Mbps and upstream rates of up to 1 Mbps. Designed for small office, home office and residential users, the router enables even faster Internet connections. You can enjoy ADSL services and broadband multimedia applications such as interactive gaming, video streaming and real-time audio much easier and faster than ever before.

BEC 7800N supports PPPoA (RFC 2364 – PPP (Point-to-Point Protocol) over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516) to establish a connection with your ISP. Your new router also supports VC-based and LLC-based multiplexing.

The perfect solution for connecting a small group of PCs to a high-speed broadband Internet connection, BEC 7800N allows multiple users to have high-speed Internet access simultaneously.

Your new router also serves as an Internet firewall, protecting your network from access by outside users. Not only does it provide a natural firewall function with Network Address Translation (NAT), it also provides rich firewall features to secure your network. All incoming data packets are monitored and filtered. You can also configure your new router to block internal users from accessing the Internet.

BEC 7800N provides two levels of security support. First, it masks LAN IP addresses making them invisible to outside users on the Internet, so it is much more difficult for a hacker to target a machine on your network. Second, it can block and redirect certain ports to limit the services that outside users can access. To ensure that games and other Internet applications run properly, you can open specific ports for outside users to access internal services on your network.

The Integrated DHCP (Dynamic Host Control Protocol) client and server services allow multiple users to get IP addresses automatically when the router boots up. Simply set local machines as a DHCP client to accept a dynamically assigned IP address from the DHCP server and reboot. Each time a local machine is powered up; the router recognizes it and assigns an IP address to instantly connect it to the LAN.

For advanced users, Virtual Service (port mapping) functions allow the product to provide limited visibility to local machines with specific services for outside users. For instance, a dedicated web server can be connected to the Internet via the router and then incoming requests for web pages that are received by the router can be rerouted to your dedicated local web server, even though the server now has a different IP address.

Virtual Server can also be used to re-task services to multiple servers. For instance, you can set the router to allow separated FTP, Web, and Multiplayer game servers to share the same Internet-visible IP address while still protecting the servers and LAN users from hackers.

Features

Express Internet Access

The router complies with ADSL worldwide standards. It supports downstream rate up to 12/24 Mbps with ADSL2/2+, 8Mbps with ADSL. Users enjoy not only high-speed ADSL services but also broadband multimedia applications such as interactive gaming, video streaming and real-time audio much easier and faster than ever. It is compliant with Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (ITU G.992.1); G.lite (ITU G.992.2); G.hs (ITU G994.1); G.dmt.bis (ITU G.992.3); G.dmt.bis. plus (ITU G.992.5)).

EWAN

Besides using ADSL to get connected to the Internet, BEC 7800N EWAN port is an alternative WAN port used to connect to Cable Modems, VDSL, fiber optic lines and PON. This alternative, yet faster method of connecting to the internet provides users with more flexibility to get online.

Fast Ethernet Switch

A 4-port 1000Mbps fast Ethernet switch is built in with automatic switching between MDI and MDI-X. An Ethernet straight or crossover cable can be used directly for auto detection.

Multi-Protocol to Establish a Connection

It supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516), and IPoA (RFC1577) to establish a connection with the ISP. The product also supports VC-based and LLC-based multiplexing.

PPP over Ethernet (PPPoE)

BEC 7800N provides an embedded PPPoE client function to establish a connection. You get greater access speed without changing the operation concept, while sharing the same ISP account and paying for one access account. No PPPoE client software is required for the local computer. Automatic Reconnect and Disconnect Timeout (Idle Timer) functions are also provided.

Universal Plug and Play (UPnP) and UPnP NAT Traversal

This protocol is used to enable simple and robust connectivity among stand-alone devices and PCs from many different vendors. It makes network simple and affordable for users. UPnP architecture leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices. With this feature enabled, users can now connect to Net meeting or MSN Messenger seamlessly.

Network Address Translation (NAT)

Allows multi-users to access outside resources such as the Internet simultaneously with one IP address/one Internet access account. Many application layer gateway (ALG) are supported

such as web browser, ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting, IP phone and others.

Domain Name System (DNS) Relay

It provides an easy way to map the domain name (a friendly name for users such as www.yahoo.com) and IP address. When a local machine sets its DNS server with this router's IP address, every DNS conversion request packet from the PC to this router will be forwarded to the real DNS in the outside network.

Dynamic Domain Name System (DDNS)

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname. This dynamic IP address is the WAN IP address. For example, to use the service, you must first apply for an account from a DDNS service like **http://www.dyndns.org/**. More than 5 DDNS servers are supported.

Virtual Server

Users can specify some services to be visible from outside users. The router can detect incoming service requests and forward either a single port or a range of ports to the specific local computer to handle it. For example, a user can assign a PC in the LAN acting as a WEB server inside and expose it to the outside network. Outside users can browse inside web servers directly while it is protected by NAT. A DMZ host setting is also provided to a local computer exposed to the outside network, Internet.

Rich Packet Filtering

Not only filters the packet based on IP address, but also based on Port numbers. It will filter packets from the Internet and vice versa, in addition to providing a higher level of security control.

Dynamic Host Configuration Protocol (DHCP) Client and Server

In the WAN site, the DHCP client can get an IP address from the Internet Service Provider (ISP) automatically. In the LAN site, the DHCP server can allocate a range of client IP addresses and distribute them including IP address, subnet mask as well as DNS IP address to local computers. It provides an easy way to manage the local IP network.

Web based GUI

It supports web based GUI for configuration and management. It is user-friendly and comes with on-line help. It also supports remote management capability for remote users to configure and manage this product.

Firmware Upgradeable

Device can be upgraded to the latest firmware through the WEB based GUI.

Chapter 2: Installing the Router

Important note for using this router

Warning

- Do not use this router in a high humidity or high temperature environment.
- Do not apply the same power source for this router to other types of equipments.
- Do not open or repair the case yourself. If the device becomes too hot, turn it off immediately and have it repaired at a qualified service center.
- Avoid using this product and all its accessories outdoor.

Attention

- Place the router on a stable surface.
- Only use the power adapter that comes with the package. Using a different voltage rating power adapter may damage the router.

Package Contents

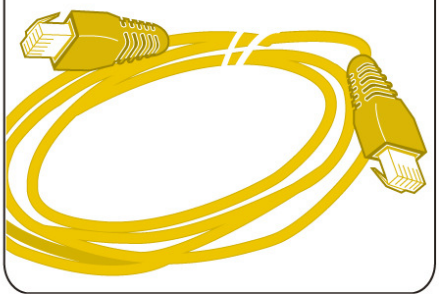
- BEC 7800(N) (802.11n) Dual WAN ADSL2+ Firewall Router
- CD containing the online manual
- RJ-11 ADSL/Telephone cable
- Ethernet (RJ-45) cable
- Three 2dBi detachable antennas (Wireless model only)
- Power adapter
- Quick Start Guide
- Splitter / Microfilter (Optional)

ADSL2+ Router

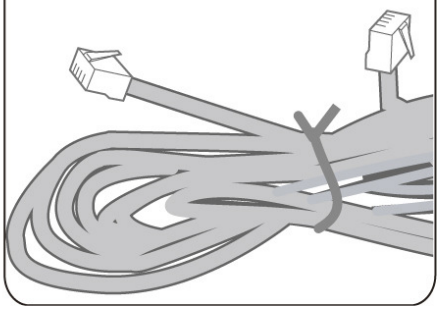
Quick Start Guide

CD

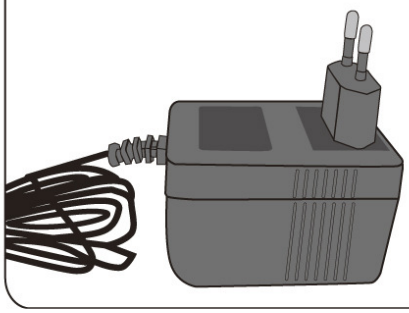
RJ-45 Ethernet cable



RJ-11 Phone cable

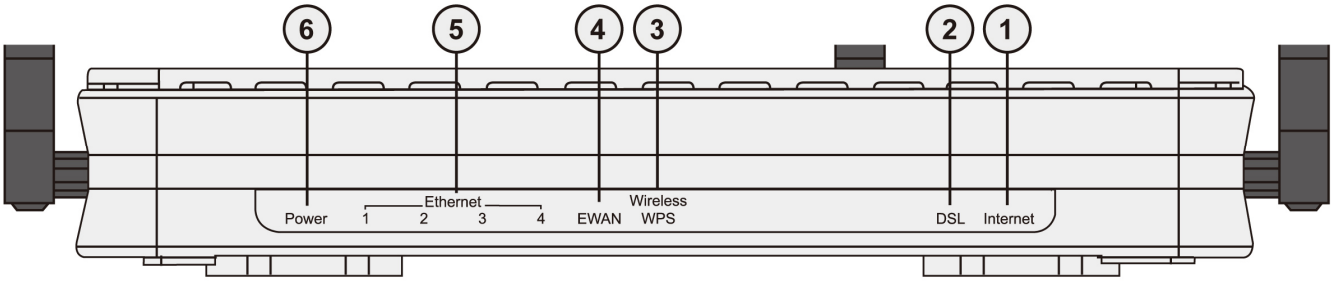


Power Adapter
(The type may differ by different country)



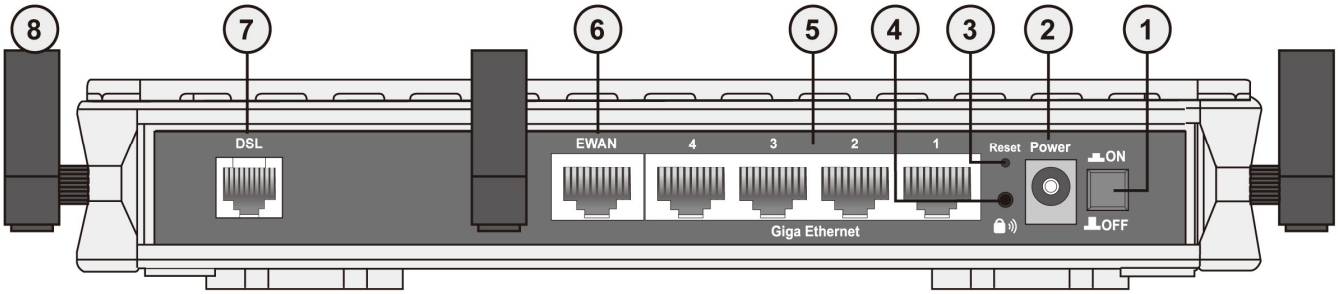
Device Description

The Front LEDs



LED		Meaning
1	**Internet**	Lit orange when WAN port fails to get IP address. Flash green when WAN port gets IP address successfully and when data is transmitted.
2	**DSL**	Lit Green when the device is successfully connected to an ADSL DSLAM. (“line sync”).
3	**Wireless / WPS**	Lit green when a wireless connection is established. Lit orange when WPS is enabled. Flash green when data is sent / received.
4	**EWAN**	Lit orange when connected to a broadband connection device. Lit orange for 10/100Mbps. Blinking when data is Transmitted / Received.
5	**Ethernet port 1X — 4X (RJ-45 connector)**	Lit orange when one of LAN ports is connected to an Ethernet device. Lit green when the speed of transmission hits 1000Mbps; Lit orange when the speed of transmission hits 10/100Mbps. Blink when data is being Transmitted / Received.
6	**Power**	When the device is booting, green light will lit while orange light will flash. When the system is ready, it will lit green. While the system is rebooting or during firmware upgrade, the LED light will flash green. Lit orange when the device fails to boot or when the device is in emergency mode.

The Rear Ports



Port		Meaning
1	**Power Switch**	Power ON/OFF switch.
2	**Power**	Connect it with the supplied power adapter.
3	**RESET**	Press more than 1 second to restore the device to its default mode.
4	**WPS**	Push WPS button to trigger Wi-Fi Protected Setup function.
5	**Giga Ethernet**	Connect to a PC or an office/home network of 10Mbps, 100Mbps or 1000Mbps using the provided RJ-45 Ethernet cables.
6	**EWAN**	WAN 10/100Mbps Ethernet port (with auto crossover support). Connect Cable Modem, VDSL, and Fiber Modem or PON optic lines with your RJ-45 cable.
7	**DSL**	Connect this port to the ADSL/telephone network with the RJ-11 cable (telephone) provided.
8	**Antenna**	Connect the detachable antenna to this port.

Cabling

One of the most common causes of problem is bad cabling or ADSL line(s). Make sure that all connected devices are turned on. On the front panel of your router is a bank of LEDs. Verify that the LAN Link and ADSL line LEDs are lit. If they are not, verify if you are using the proper cables.

Make sure that all devices (e.g. telephones, fax machines, analogue modems) connected to the same telephone line as your router have a line filter connected between them and the wall outlet (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and that all line filters are correctly installed in a right way. If line filter is not installed and connected properly, it may cause problem to your ADSL connection or may result in frequent disconnections.

Chapter 3: Basic Installation

The router can be configured through your web browser. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista, etc. The product provides an easy and user-friendly interface for configuration.

Please check your PC network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

There are ways to connect the router, either through an external repeater hub or connect directly to your PCs. However, make sure that your PCs have an Ethernet interface installed properly prior to connecting the router device. You ought to configure your PCs to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is 192.168.1.254 and the subnet mask is 255.255.255.0 (i.e. any attached PC must be in the same subnet, and have an IP address in the range of 192.168.1.100 to 192.168.1.199). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problem accessing the router web interface it is advisable to uninstall your firewall program on your PCs, as they can cause problems accessing the IP address of the router. Users should make their own decisions on what is best to protect their network.

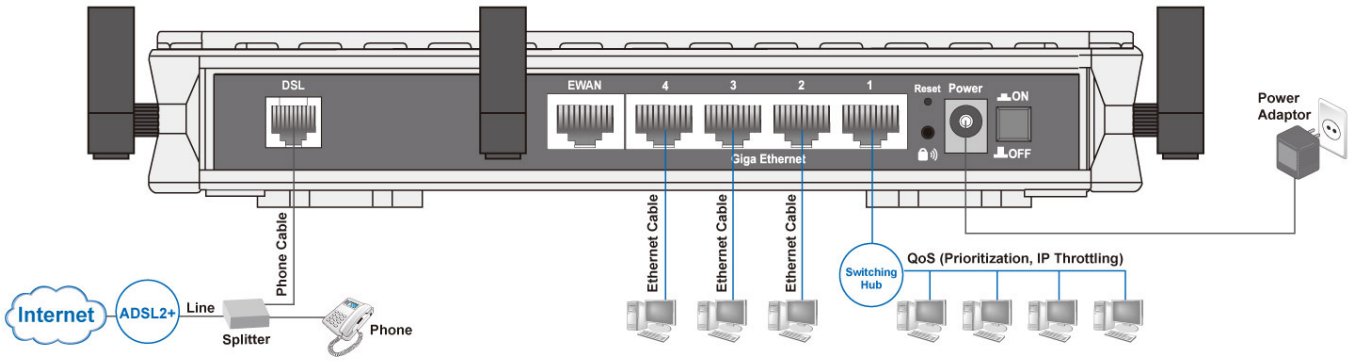
Please follow the following steps to configure your PC network environment.

Any TCP/IP capable workstation can be used to communicate with or through this router. To configure other types of workstations, please consult your manufacturer documentation.

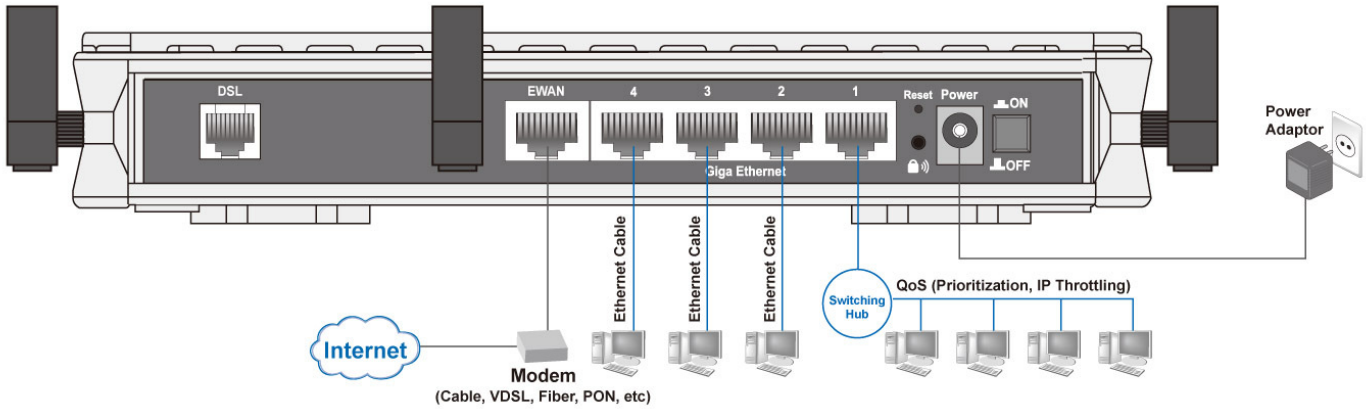
Connecting Your Router

Users will not be able to connect to the internet through EWAN if DSL is already connected to the internet. Only one connection type (EWAN or DSL) is allowed to connect to the internet at one time.

ADSL Router Mode



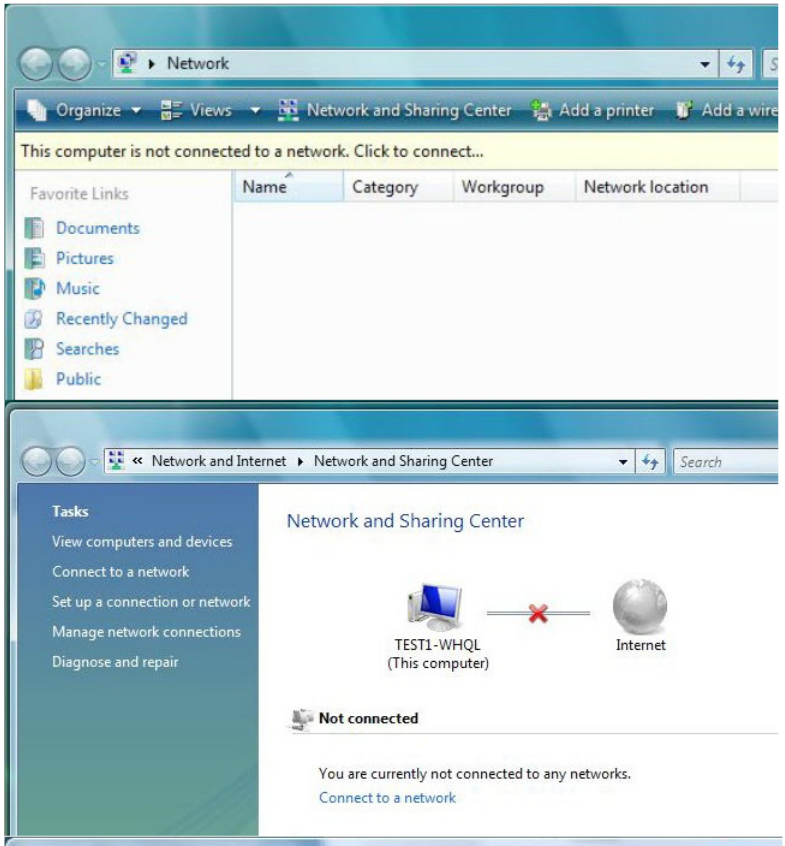
Broadband Router Mode



Network Configuration

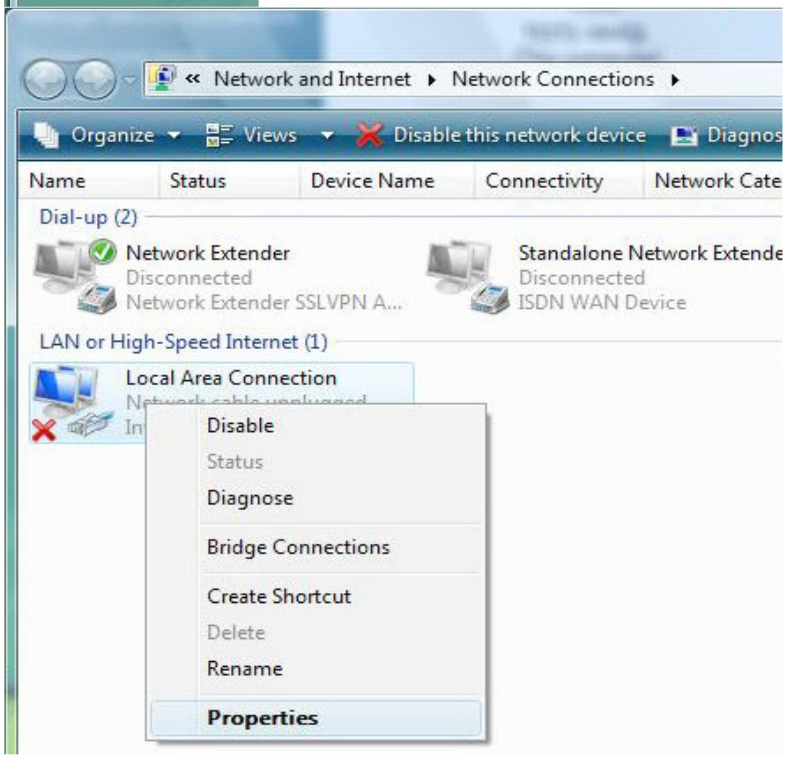
Configuring PC in Windows Vista

1. Go to Start. Click on Network.
2. Then click on Network and Sharing Center at the top bar.

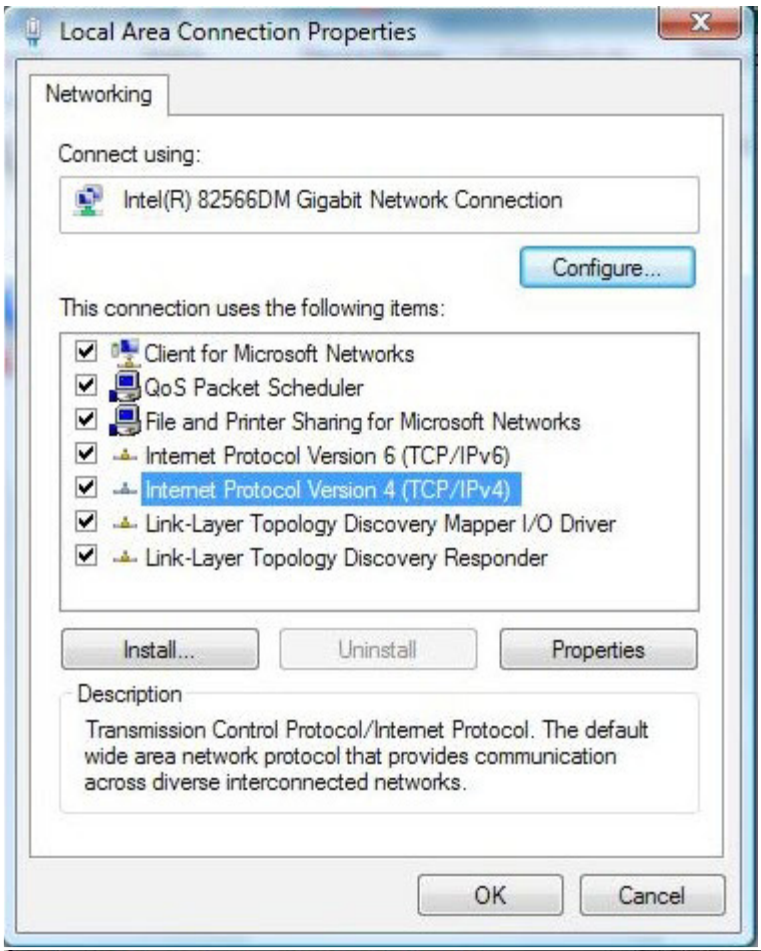


3. When the Network and Sharing Center window pops up, select and click on Manage network connections on the left window column.

4. Select the Local Area Connection, and right click the icon to select Properties.

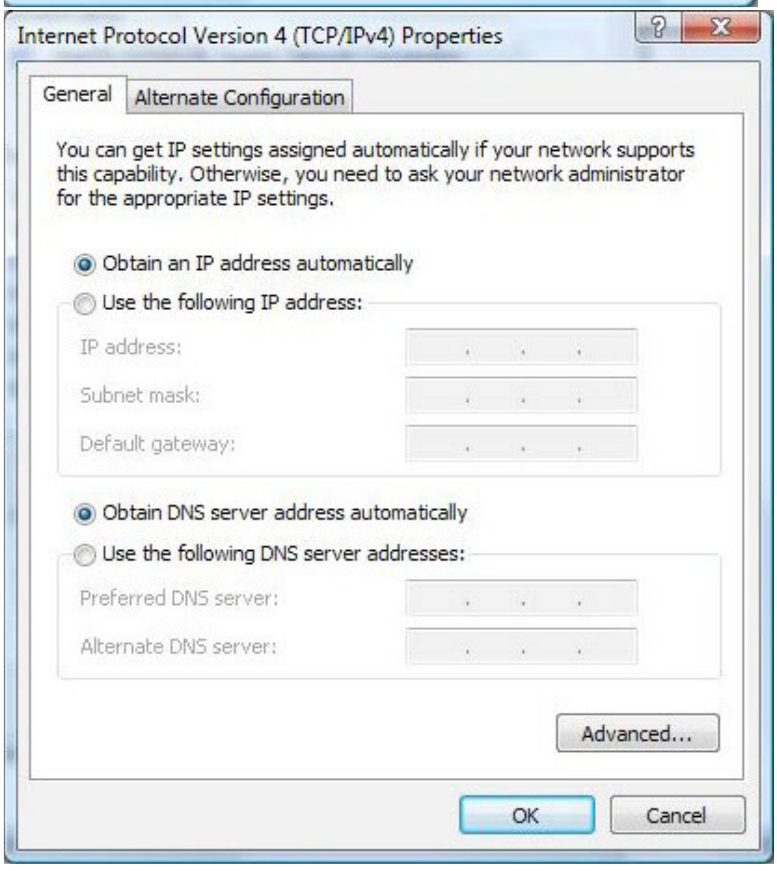


5. Select Internet Protocol Version 4 (TCP/IPv4) then click Properties.



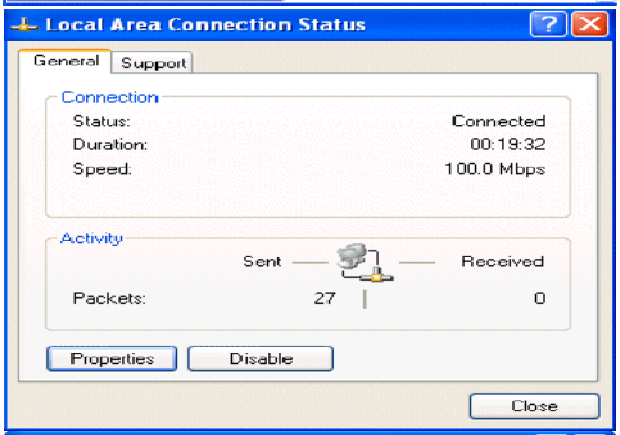
6. In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting.

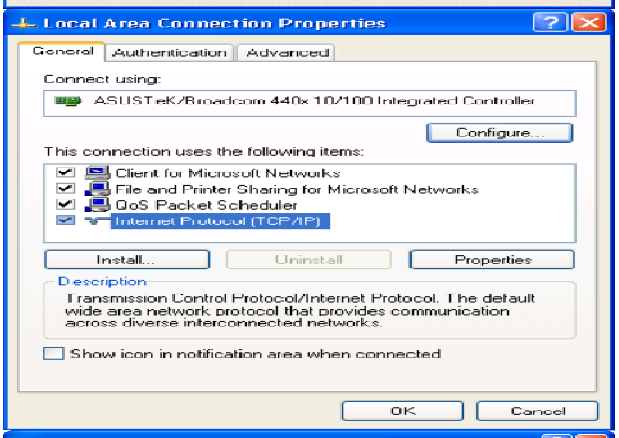
7. Click OK again in the Local Area Connection Properties window to apply the new configuration.

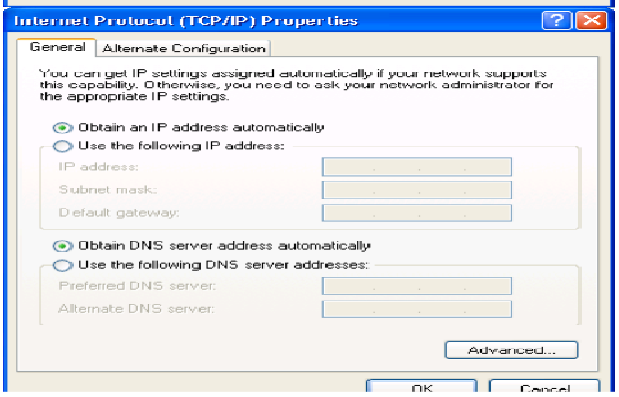

Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Configuring PC in Windows XP

1. Go to Start > Control Panel (in Classic View). In the Control Panel, double-click on Network Connections
2. Double-click Local Area Connection.
3. In the Local Area Connection Status window, click Properties.
4. Select Internet Protocol (TCP/IP) and click Properties.
5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.
6. Click OK to finish the configuration.

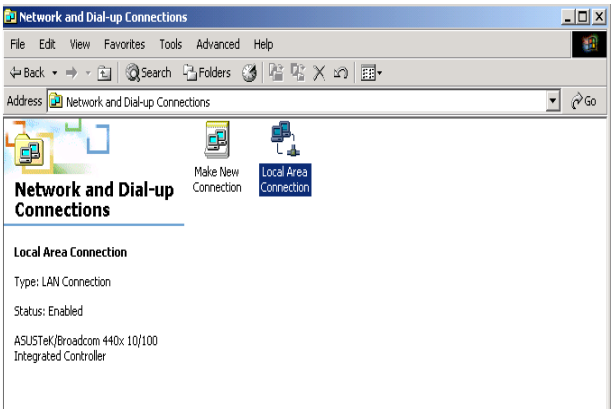



Local Area Connection Properties
General Authentication Advanced
Connect using:
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol (TCP/IP)
Install... Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
OK Cancel

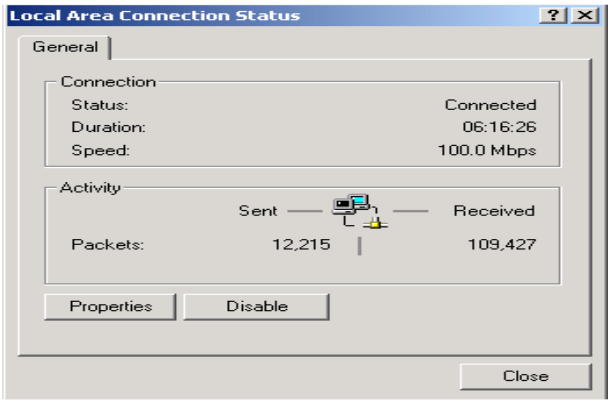

Internet Protocol (TCP/IP) Properties
General Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK Cancel

Configuring PC in Windows 2000

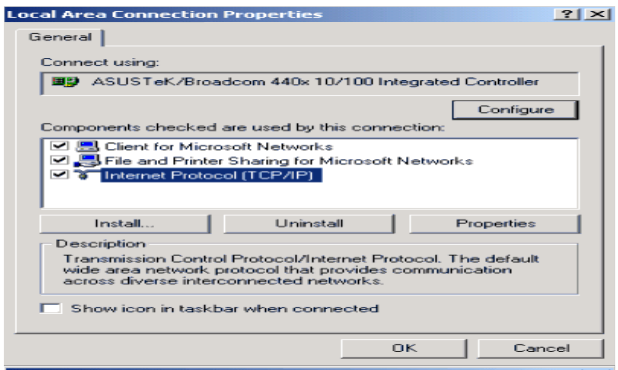
1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and Dial-up Connections.
2. Double-click Local Area Connection.



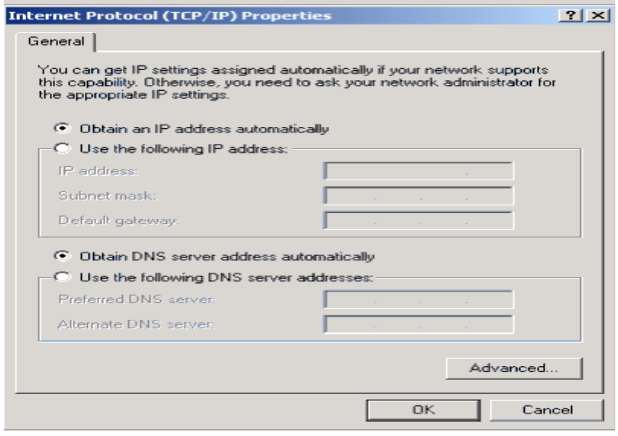
3. In the Local Area Connection Status window click Properties.



4. Select Internet Protocol (TCP/IP) and click Properties.

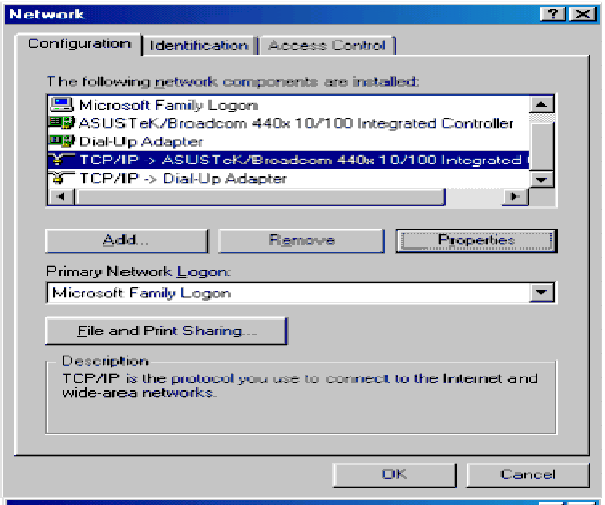


5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.
6. Click OK to finish the configuration.

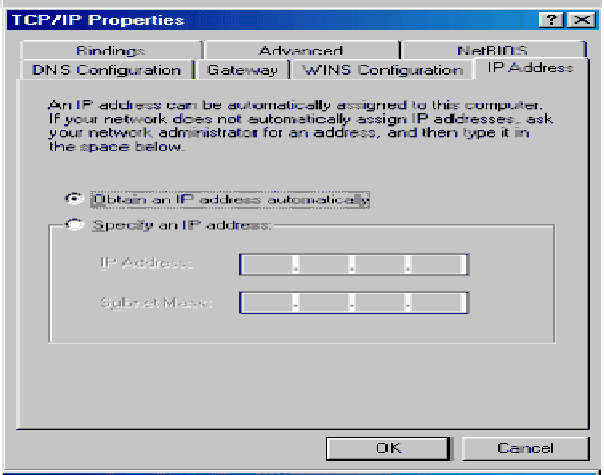

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Configuring PC in Windows 95/98/Me

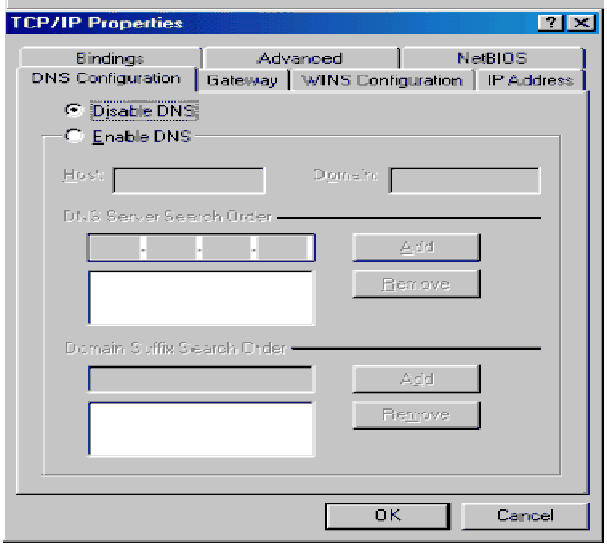
1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and choose the Configuration tab.
2. Select TCP/IP > NE2000 Compatible, or the name of your Network Interface Card (NIC) in your PC.



3. Select the Obtain an IP address automatically radio button.

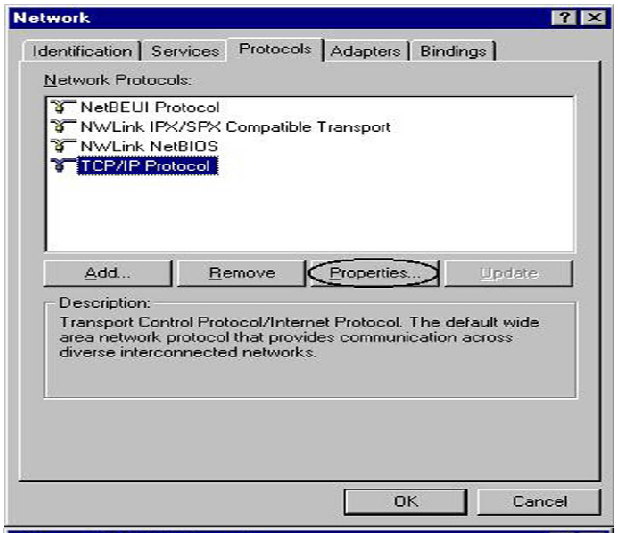

TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

4. Then select the DNS Configurationtab.
5. Select the Disable DNS radio button and click OK to finish the configuration.

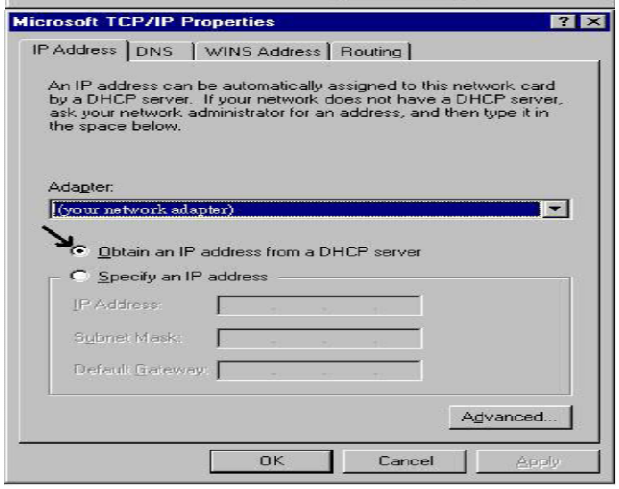


Configuring PC in Windows NT4.0

1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and choose the Protocols tab.
2. Select TCP/IP Protocol and click Properties.



3. Select the Obtain an IP address from a DHCP server radio button and click OK.


Microsoft TCP/IP Properties
IP Address
DNS
WINS Address
Routing
An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.
Adapter:
(your network adapter)
Obtain an IP address from a DHCP server
Specify an IP address
IP Address:
Subnet Mask:
Default Gateway:
Advanced...
OK
Cancel
Apply

Factory Default Settings

Before configuring your router, you need to know the following default settings.

Web Interface (Username and Password)

- Username: admin
- Password: admin

The default username and password are “**admin**” and “**admin**” respectively.

Attention

If you have forgotten your username or password for the router, you can restore your device to its default setting by pressing the Reset button for more than 1 second.

Device LAN IP settings

- IP Address: 192.168.1.254
- Subnet Mask: 255.255.255.0

ISP setting in WAN site

- PPPoE

DHCP server

- DHCP server is enabled.
- Start IP Address: 192.168.1.100
- IP pool counts: 100

LAN and WAN Port Addresses

The parameters of LAN and WAN ports are pre-set in the factory. The default values are shown in the tale.

	LAN Port	WAN Port
IP address	192.168.1.254	The PPPoE function is enabled to automatically get the WAN port configuration from the ISP.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199	

Information from your ISP

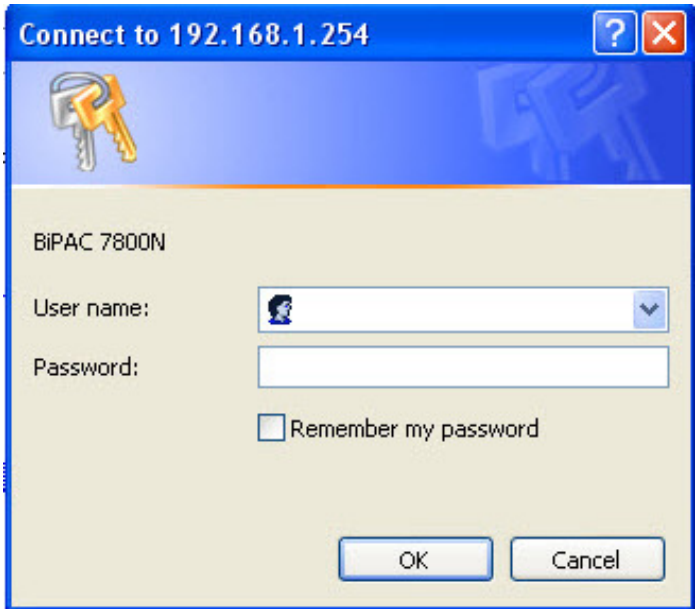
Before configuring this device, you have to check with your ISP (Internet Service Provider) to find out what kind of service is provided such as DHCP (Obtain an IP Address Automatically, Static IP (Fixed IP Address) or PPPoE.

Gather the information as illustrated in the following table and keep it for reference.

PPPoE(RFC2516)	VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
PPPoA(RFC2684)	VPI/VCI, VC / LLC-based multiplexing, Username, Password and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
MPoA(RFC1483/ RFC2684)	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).
IPoA(RFC1577)	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).
Pure Bridge	VPI/VCI, VC / LLC-based multiplexing to use Bridged Mode.

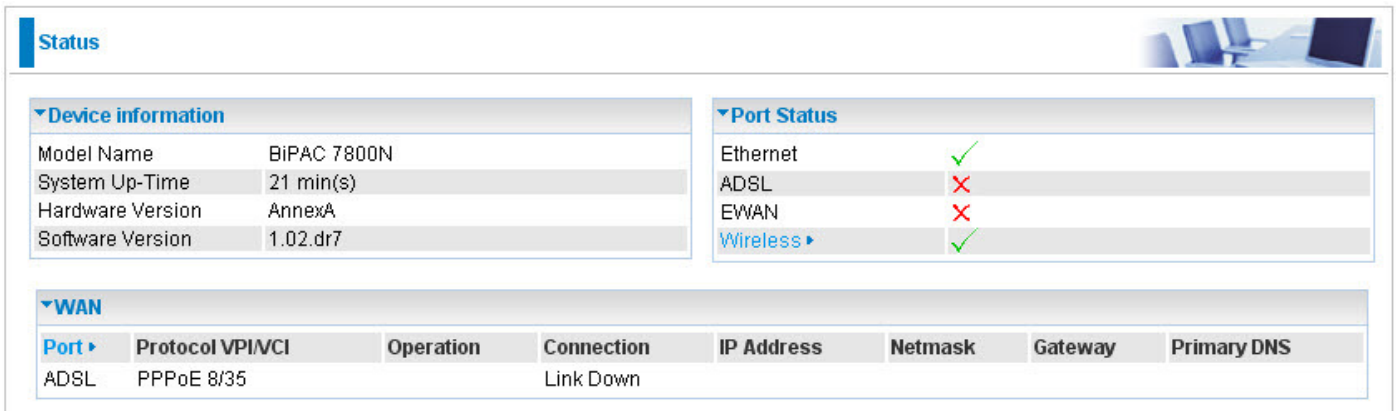
Chapter 4: Configuration

Open your web browser, enter the IP address of your router, which by default is 192.168.1.254, and click “Go”, a login window prompt will appear. The default username and password are “admin” and “admin” respectively.

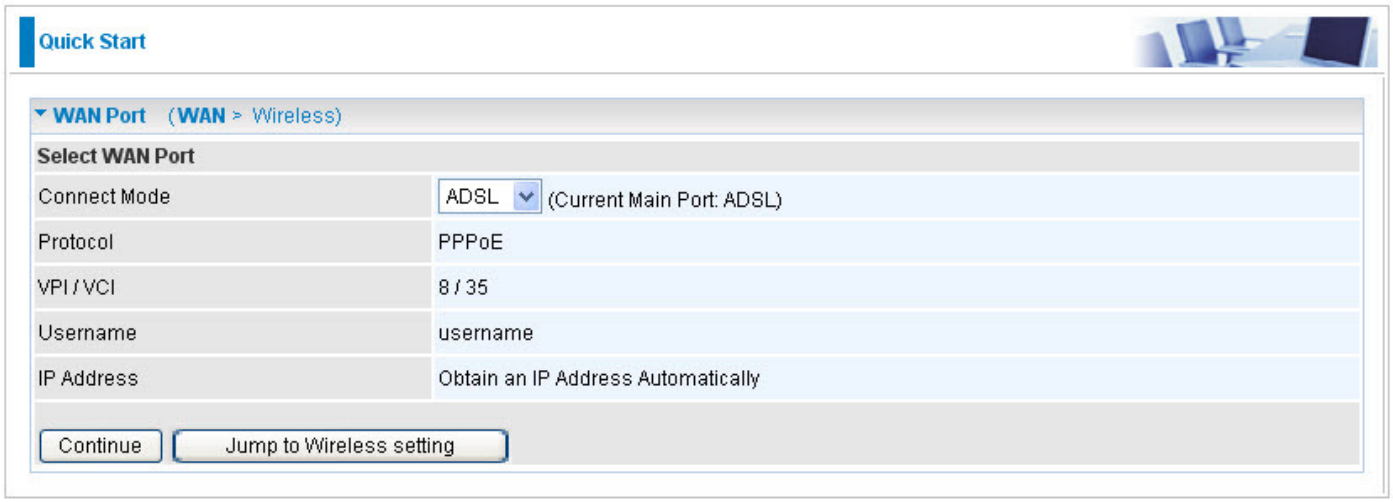


Congratulations! You are now successfully logon to the BEC 7800N Firewall Router!

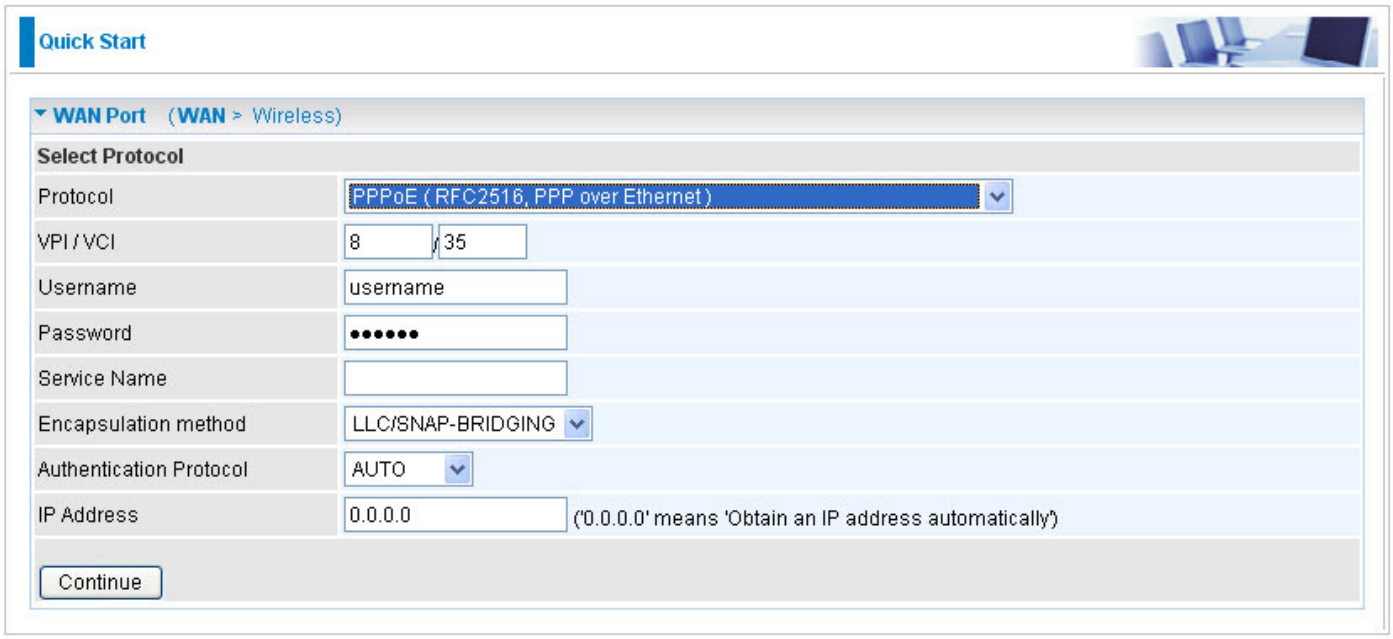
If the authentication succeeds, the homepage “Device Info - Summary” will appear on the screen.



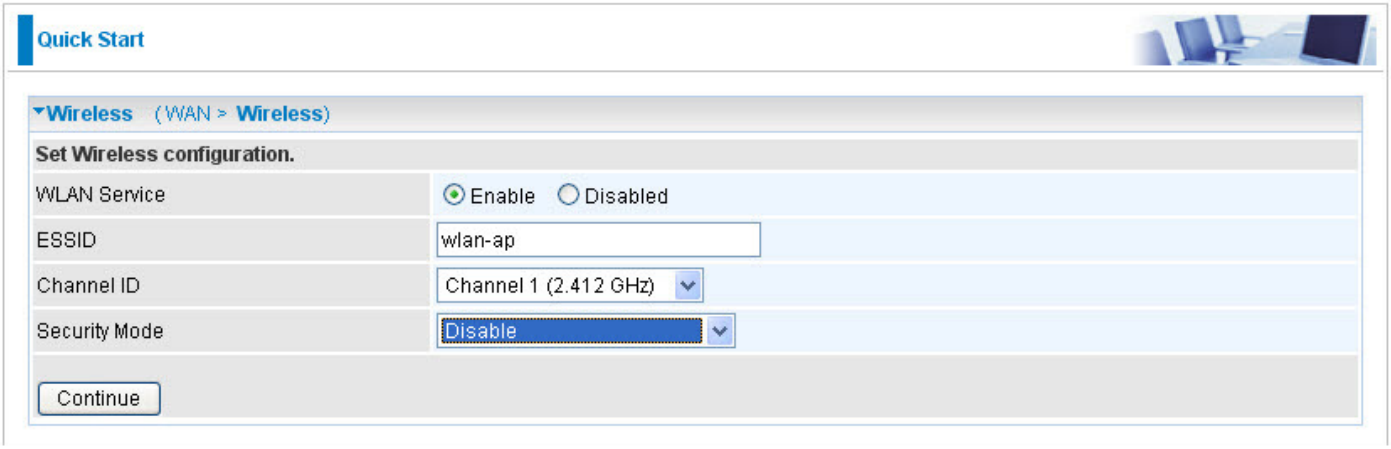
Quick Start



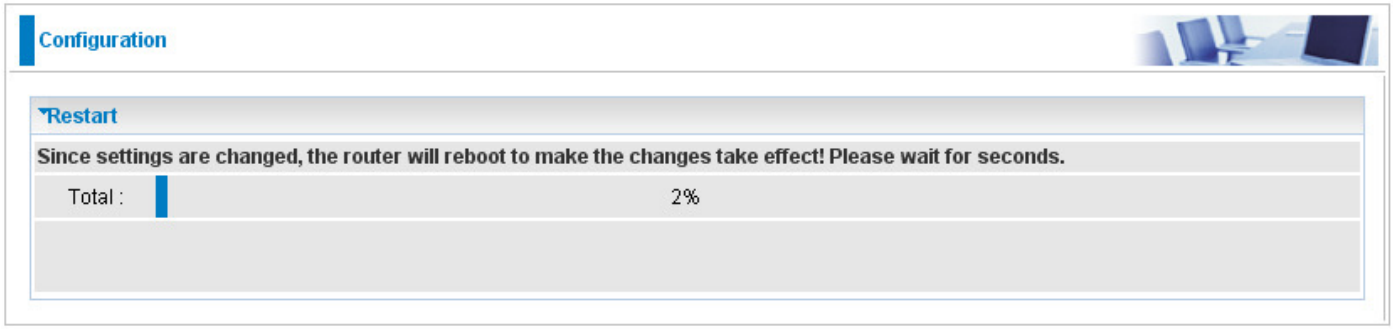
Step 1: Select WAN port connect mode from the connect mode drop down menu. There are two types of connect mode to choose from: ADSL or EWAN



Step 2: After selecting the connect mode, press Continue to move on to the next configuring page. There are 5 types of connection protocols available under ADSL connect mode while there are 2 types of connection protocols available for EWAN connect mode. ***Each type of connection mode is described in the following sections of ADSL Connect mode and EWAN Connect mode.***



Step 3: After finishing configuring the WAN port connection, you may proceed to configure the Wireless setting. There are 4 types of security mode: WPA-PSK, WPA2-PSK, WPA/WPA2 Preshared Key & WEP. Please refer to the Wireless Setting Mode section for detail description of each security mode.

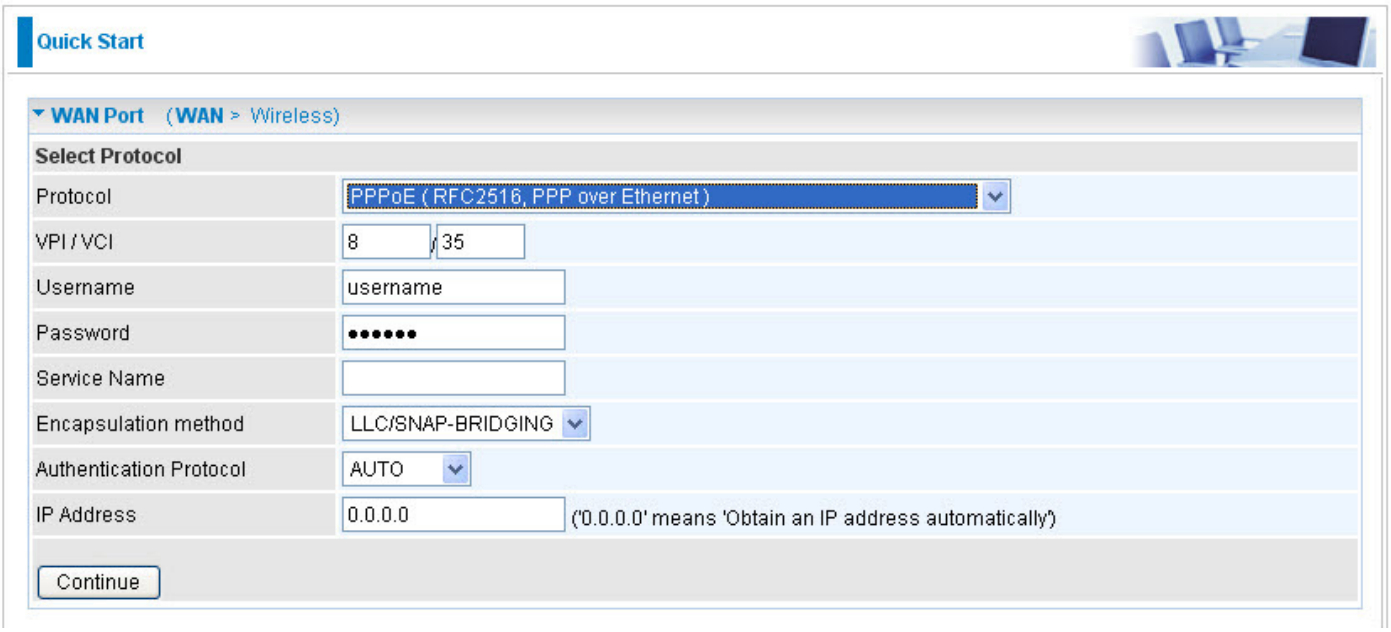

Configuration
Restart
Since settings are changed, the router will reboot to make the changes take effect! Please wait for seconds.
Total :
2%

Step 4: After finishing configuring the WAN connection, press Continue to finish the QuickStart.

ADSL Connect Mode

For ADSL connect mode there are 5 types of connection protocols: **PPPoE, PPPoA, IPoA, MPoA** and **Pure Bridge**.

PPPoE



VPI/VCI: Enter the information provided by your ISP.

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

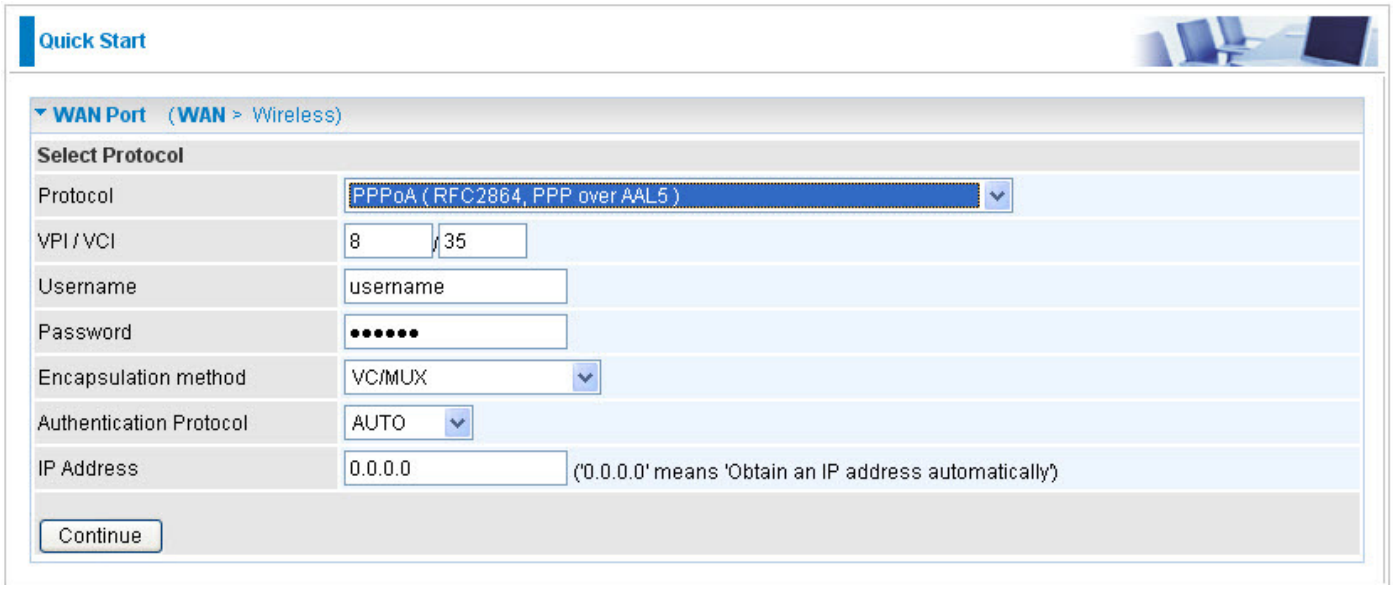
Service Name: This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

Encapsulation method: Select the encapsulation format. Select the one provided by your ISP.

Authentication method: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

IP Address: Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

PPPoA



VPI/VCI: Enter the information provided by your ISP.

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.

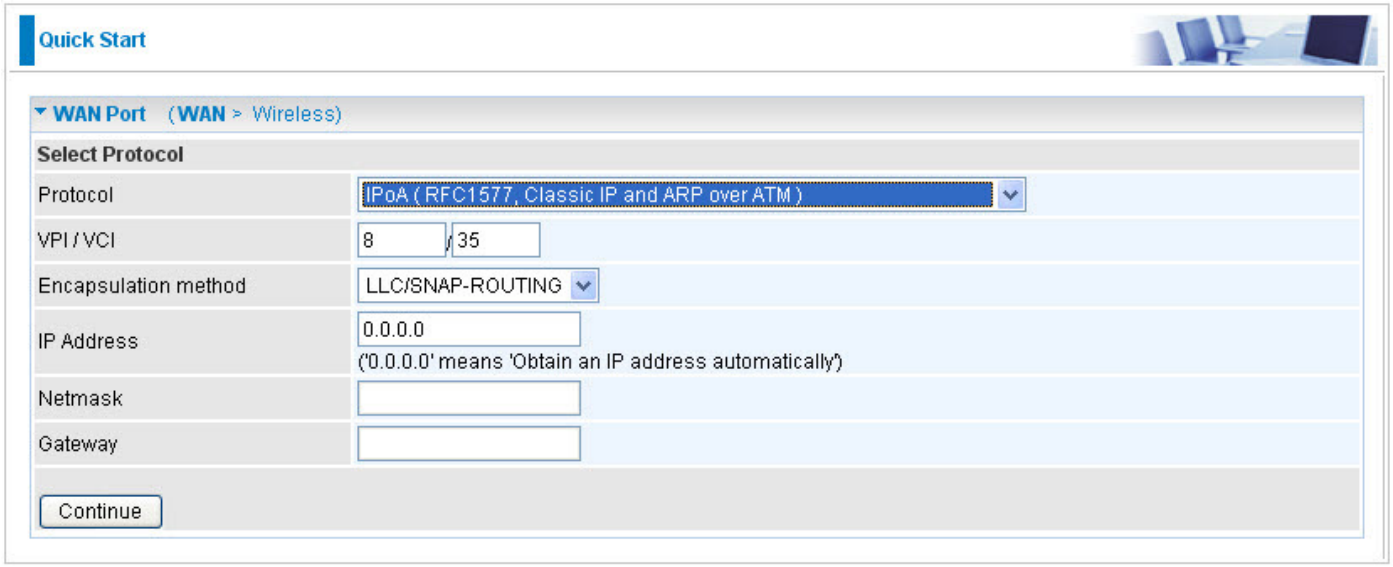
Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Encapsulation method: Select the encapsulation format. Select the one provided by your ISP.

Authentication method: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

IP Address: Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

IPoA Connection



VPI/VCI: Enter the VPI and VCI information provided by your ISP.

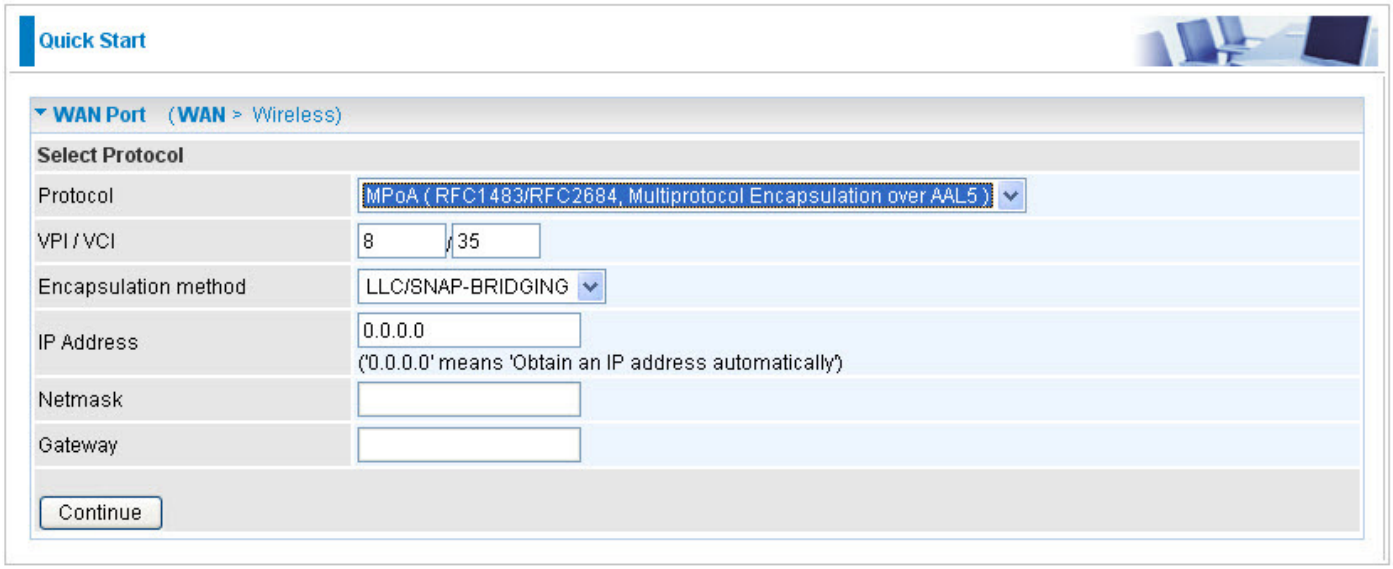
Encapsulation method: Select the encapsulation format. Select the one provided by your ISP.

IP Address: IPOA WAN IP address can only set fix IP address. If the IP is set to 0.0.0.0 (auto IP detect), both netmask and gateway may be left blank.

Netmask: User can change it to others such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given).

Gateway: Enter the IP address of the default gateway.

MPoA Connection



VPI/VCI: Enter the VPI and VCI information provided by your ISP.

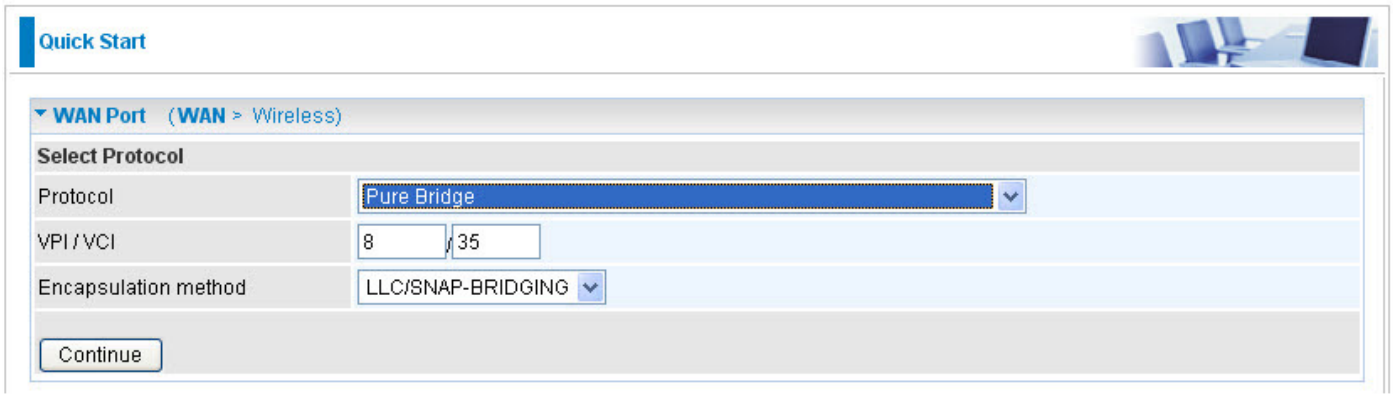
Encapsulation method: Select the encapsulation format. Select the one provided by your ISP.

IP Address: Your WAN IP address. If the IP is set to 0.0.0.0 (auto IP detect), both netmask and gateway may be left blank.

Netmask: User can change it to others such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given).

Gateway: Enter the IP address of the default gateway.

Pure Bridge connection

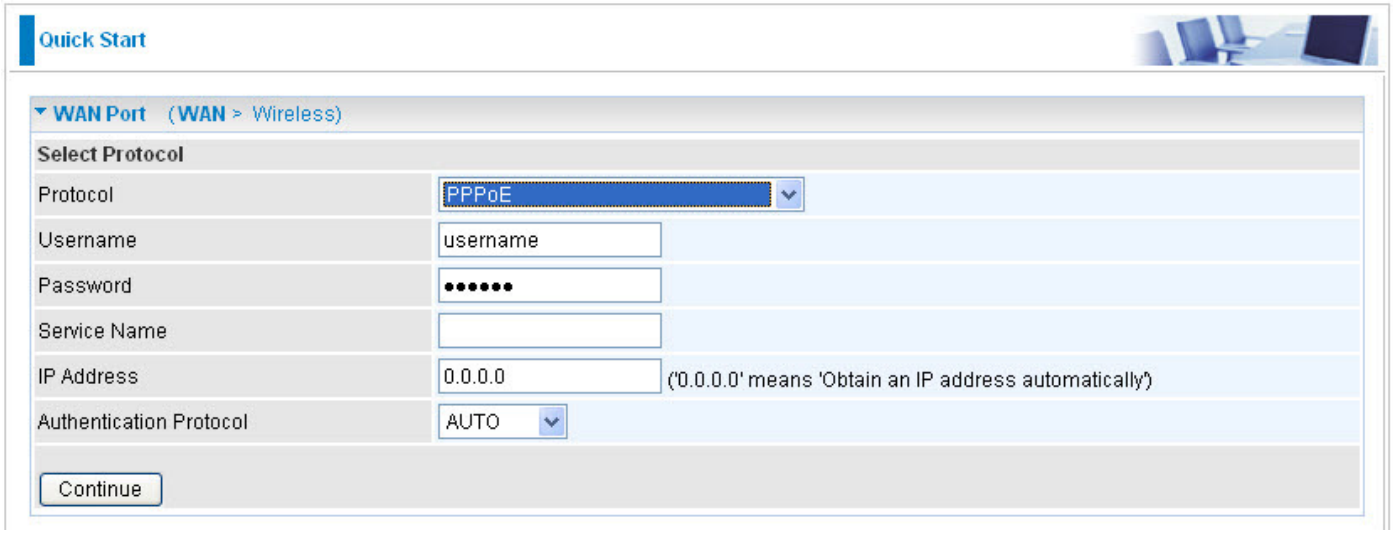


VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Encapsulation method: Select the encapsulation format. Select the one provided by your ISP.

EWAN Connect Mode

PPPoE connection



Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

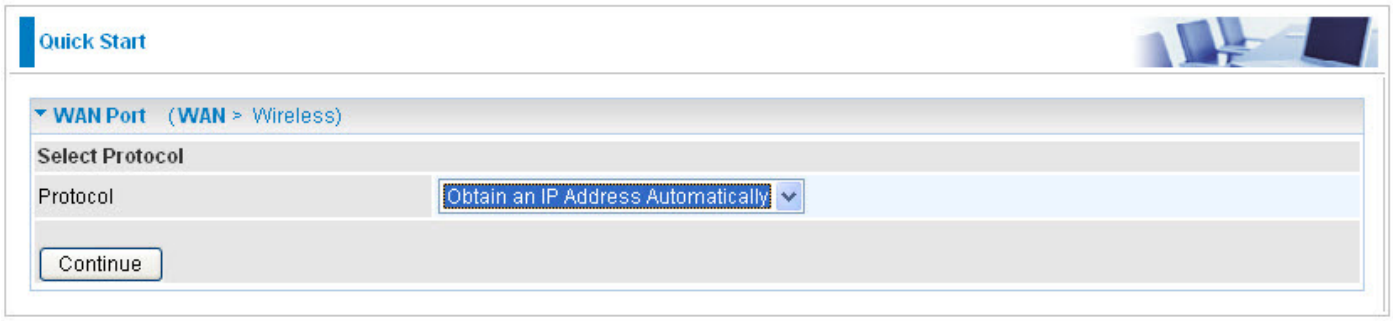
Service Name: This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

IP Address: Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

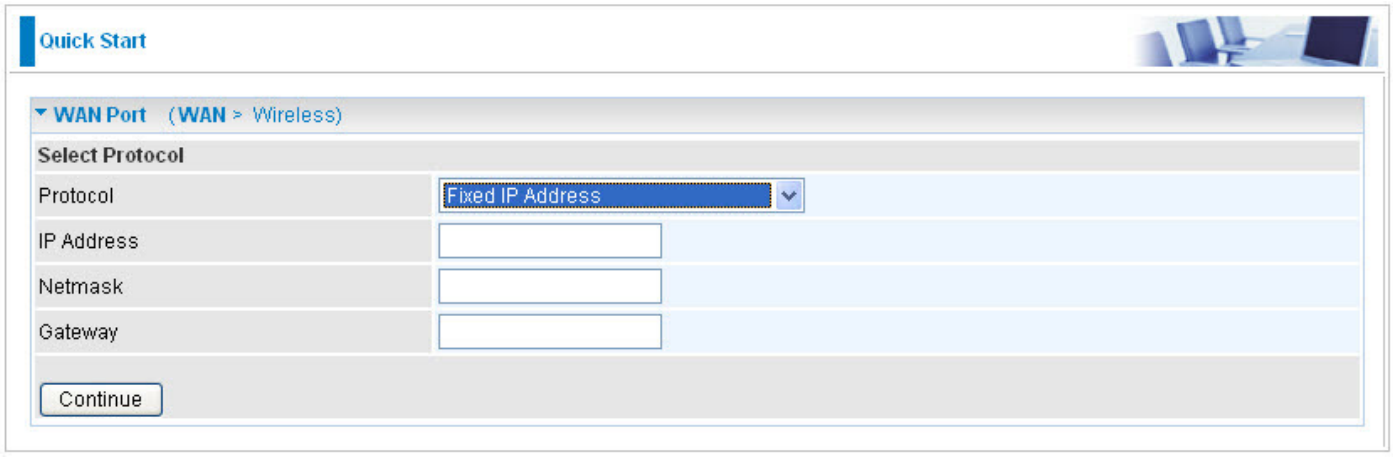
Authentication Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

Obtain an IP Address Automatically

Select this protocol enables the device to automatically retrieve IP address.



Fixed IP Address



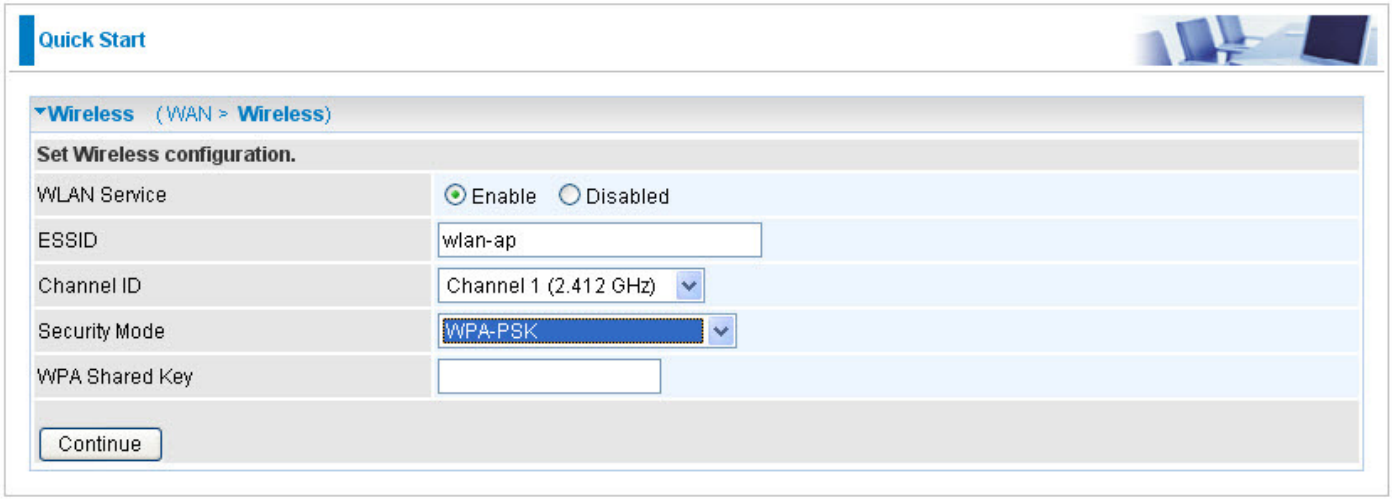
IP Address: Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

Netmask: User can change it to others such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given).

Gateway: Enter the IP address of the default gateway.

Wireless Setting Mode

WPA-PSK / WPA2-PSK



WLAN Service: Default setting is set to Enable. If you want to use wireless, you can select Enable.

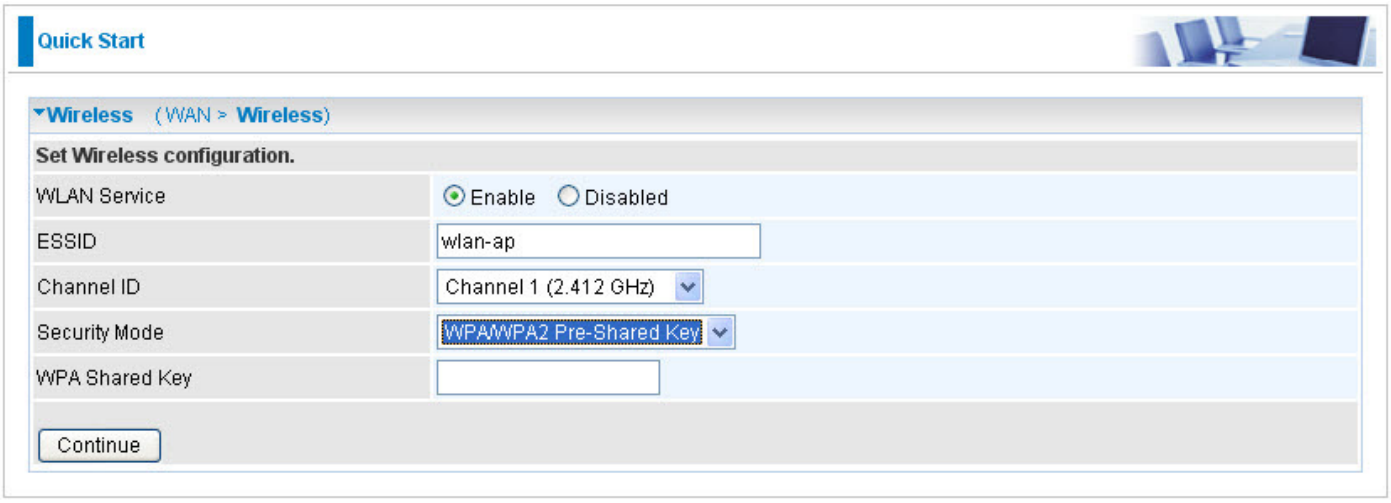
ESSID: The ESSID is the unique name of a wireless access point (AP) to be distinguished from another. For security propose, change to a unique ID name to the AP which is already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the ESSID as the device, in order to get connected to your network.

Channel ID: Select the channel ID that you would like to use.

Security Mode: You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

WPA/WPA2 Pre-shared Key



WLAN Service: Default setting is set to Enable. If you want to use wireless, you can select Enable.

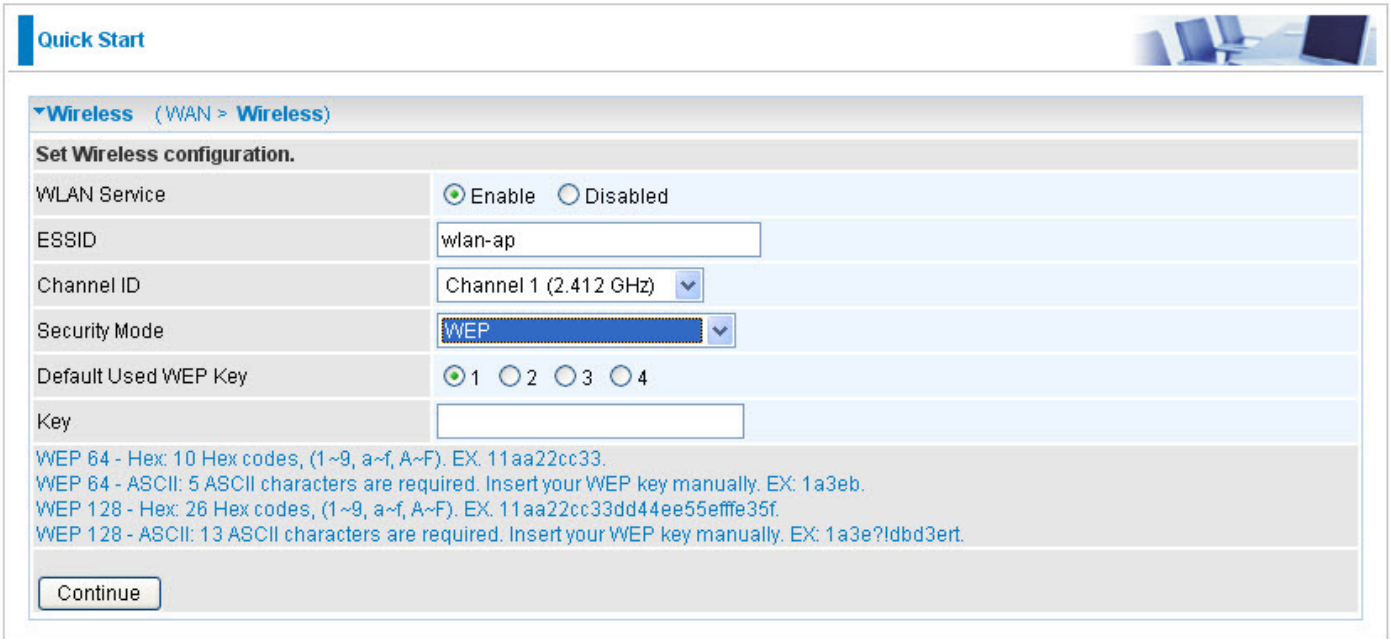
ESSID: The ESSID is the unique name of a wireless access point (AP) to be distinguished from another. For security propose, change to a unique ID name to the AP which is already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the ESSID as the device, in order to get connected to your network.

Channel ID: Select the channel ID that you would like to use.

Security Mode: You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

WEP


Quick Start
Wireless (WAN > Wireless)
Set Wireless configuration.
WLAN Service
Enable
Disabled
ESSID
wlan-ap
Channel ID
Channel 1 (2.412 GHz)
Security Mode
WEP
Default Used WEP Key
1
2
3
4
Key
WEP 64 - Hex: 10 Hex codes, (1~9, a~f, A~F). EX. 11aa22cc33.
WEP 64 - ASCII: 5 ASCII characters are required. Insert your WEP key manually. EX: 1a3eb.
WEP 128 - Hex: 26 Hex codes, (1~9, a~f, A~F). EX. 11aa22cc33dd44ee55efffe35f.
WEP 128 - ASCII: 13 ASCII characters are required. Insert your WEP key manually. EX: 1a3e?ldbd3ert.
Continue

WLAN Service: Default setting is set to Enable. If you want to use wireless, you can select Enable.

ESSID: The ESSID is the unique name of a wireless access point (AP) to be distinguished from another. For security propose, change to a unique ID name to the AP which is already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the ESSID as the device, in order to get connected to your network.

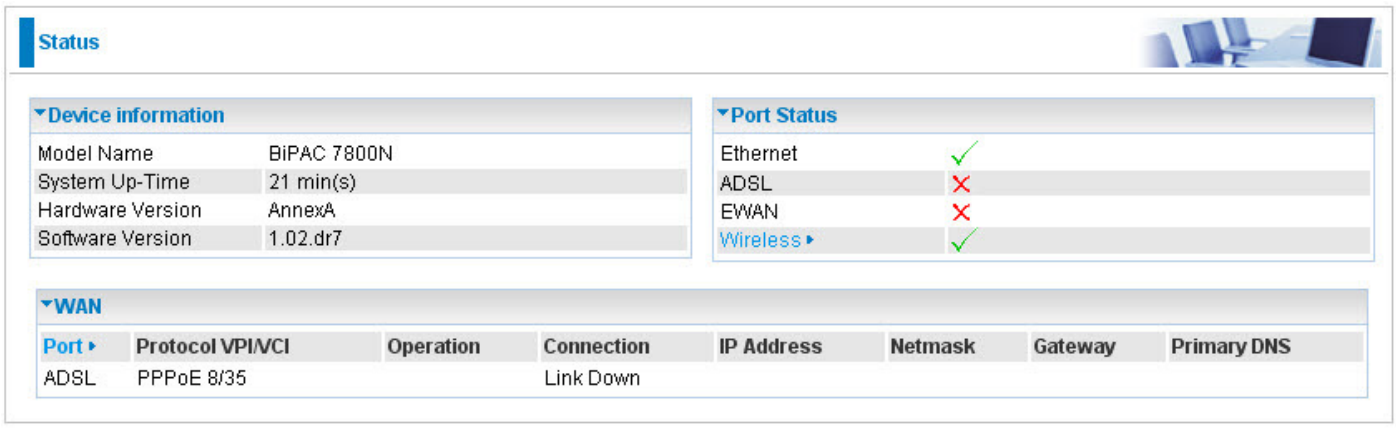
Channel ID: Select the channel ID that you would like to use.

Security Mode: You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**.

Default Used WEP Key: Select the encryption key ID; please refer to **Key (1~4)** below.

Key (1-4): Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX style, 10 and 26 HEX codes are required for WEP64 and WEP128 respectively.

Status (Basic Mode)



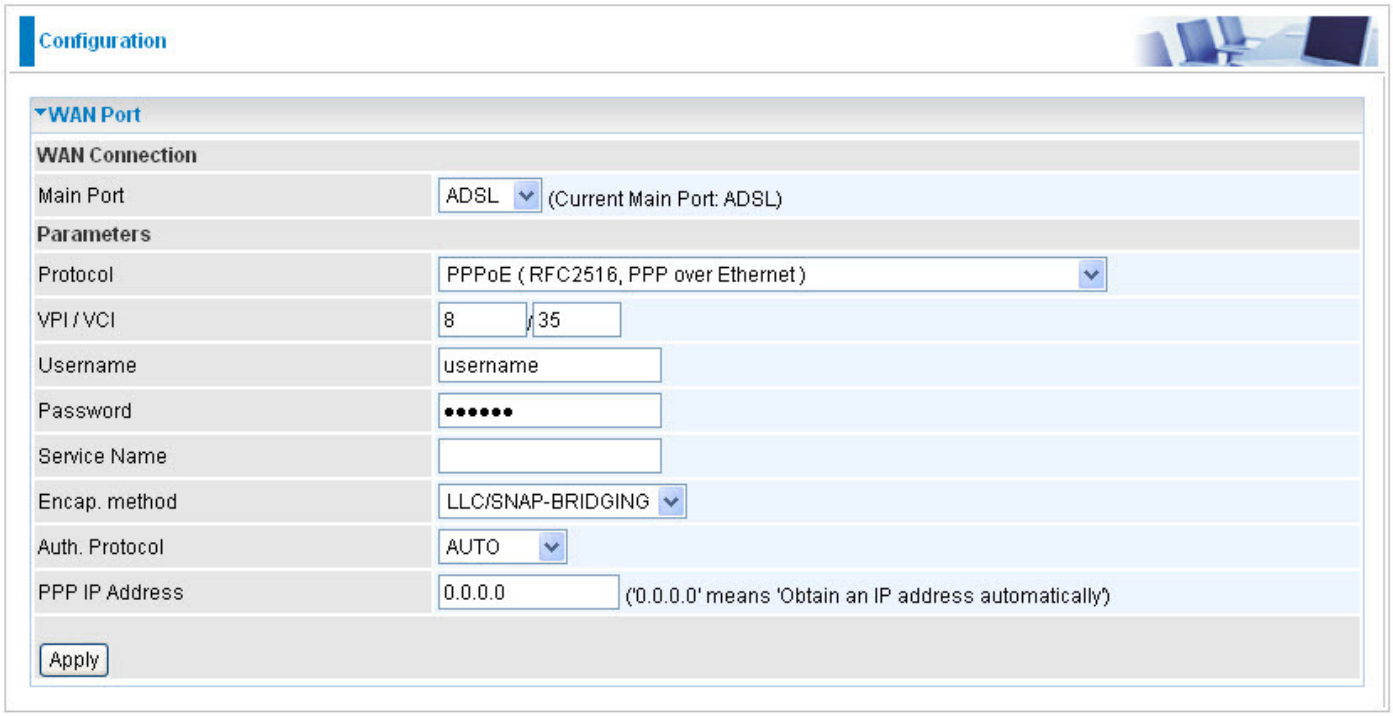
Cofiguration (Basic Mode)

A WAN (Wide Area Network) is an outside connection to another network or the Internet. There are two items within the WAN section: **WAN Profile** and **ADSL Mode**.

WAN – Main Port (ADSL)

PPPoE Connection (ADSL)

PPPoE (PPP over Ethernet) provides access control in a manner similar to dial-up services using PPP.



VPI/VCI: Enter the information provided by your ISP.

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

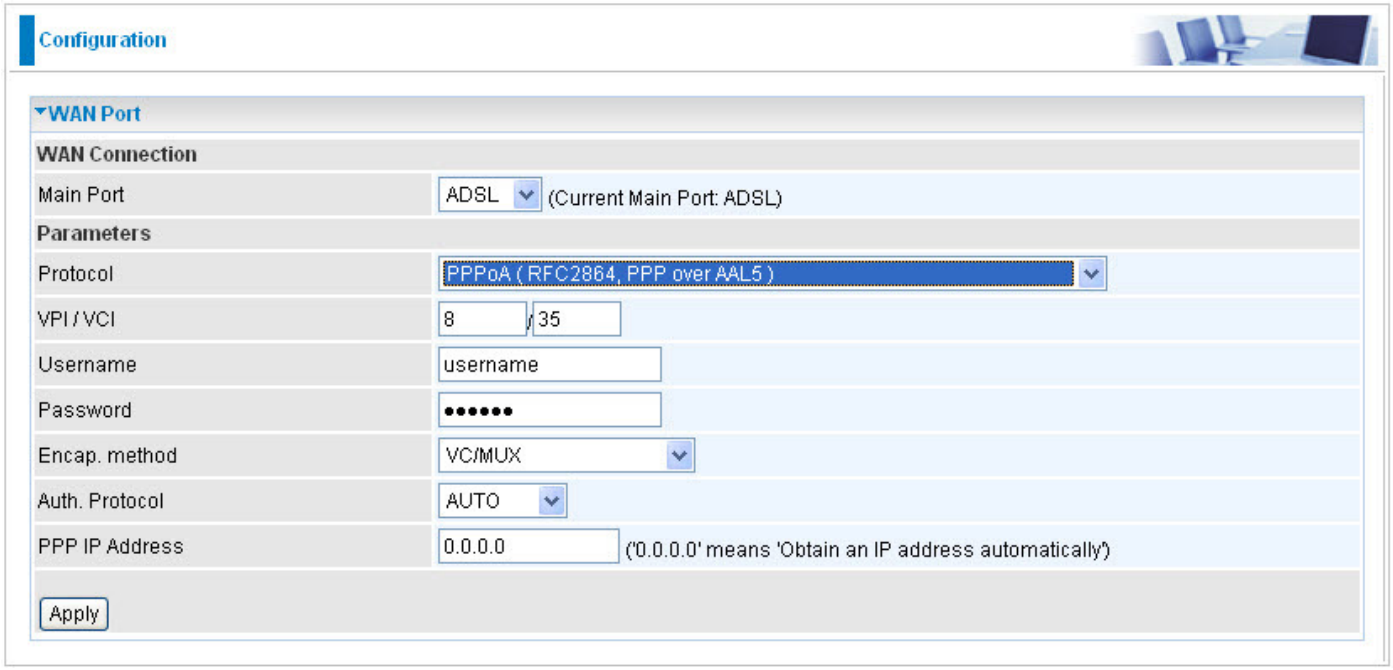
Encap. method: Select the encapsulation format. Select the one provided by your ISP.

Auth. Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

PPP IP Address(0.0.0.0:Auto): Your WAN IP address. Leave this at 0.0.0.0 to obtain automatically an IP address from your ISP.

PPPoA Connection (ADSL)

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). It provides access control and billing functionality in a manner similar to dial-up services using PPP.



VPI/VCI: Enter the information provided by your ISP.

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.

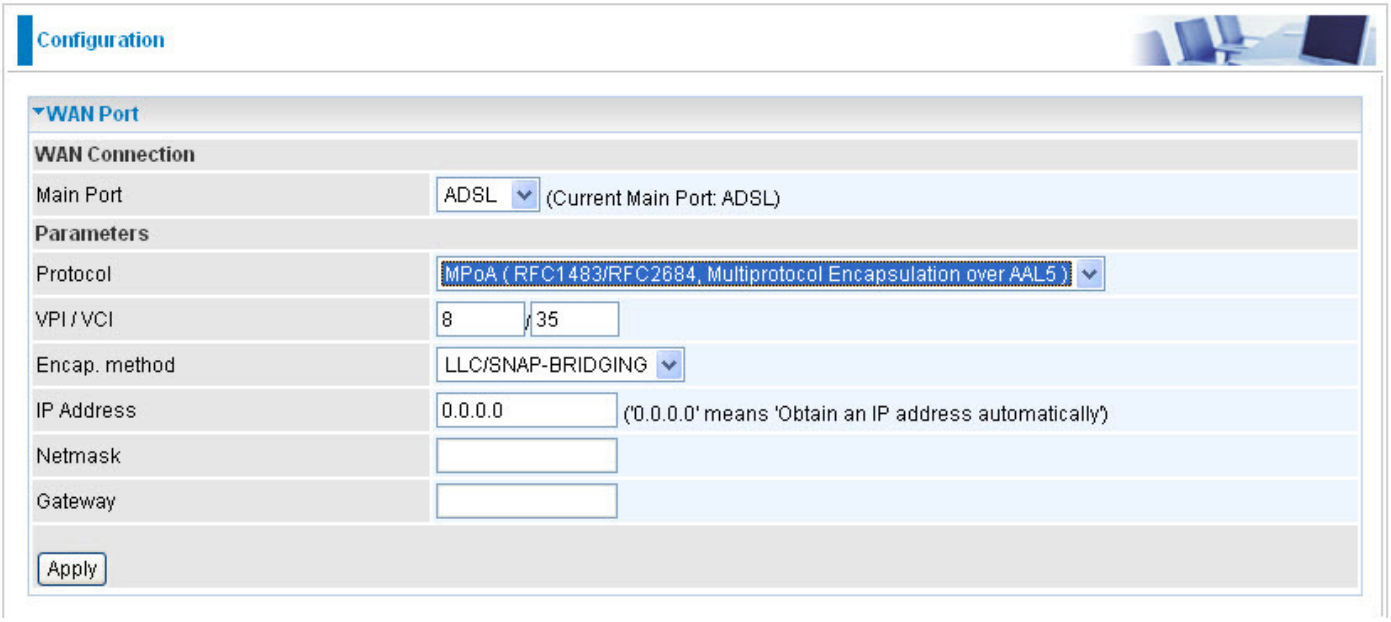
Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

Auth. Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

PPP IP Address(0.0.0.0:Auto): Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

MPoA Connection (ADSL)



VPI/VCI: Enter the VPI and VCI information provided by your ISP.

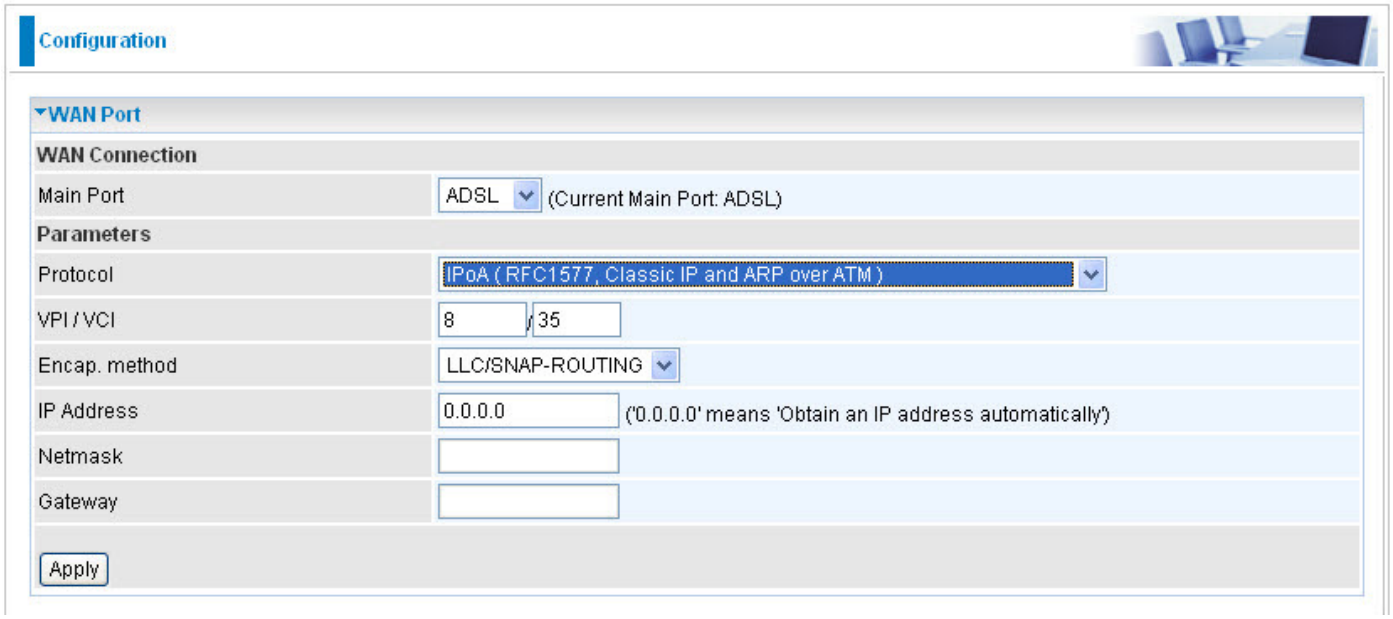
Encap. method: Select the encapsulation format. Select the one provided by your ISP.

IP Address: Your WAN IP address. If the IP is set to 0.0.0.0 (auto IP detect), both netmask and gateway may be left blank.

Netmask: User can change it to others such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given).

Gateway: Enter the IP address of the default gateway.

IPoA Connections (ADSL)



VPI/VCI: Enter the VPI and VCI information provided by your ISP.

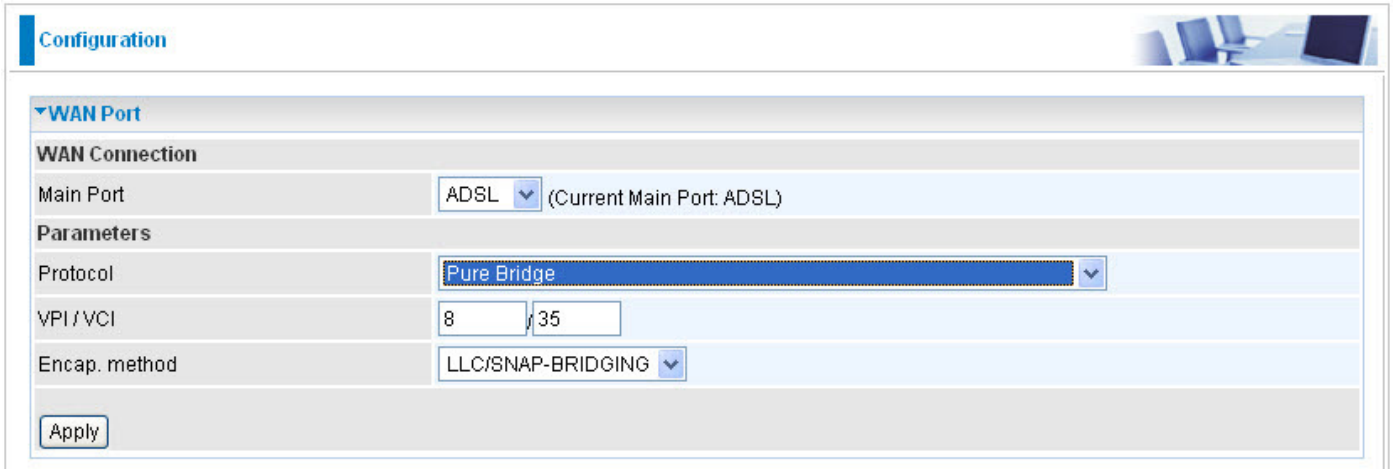
Encap. method: Select the encapsulation format. Select the one provided by your ISP.

IP Address: Your WAN IP address. If the IP is set to 0.0.0.0 (auto IP detect), both netmask and gateway may be left blank.

Netmask: User can change it to others such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given).

Gateway: Enter the IP address of the default gateway.

Pure Bridge Connections (ADSL)



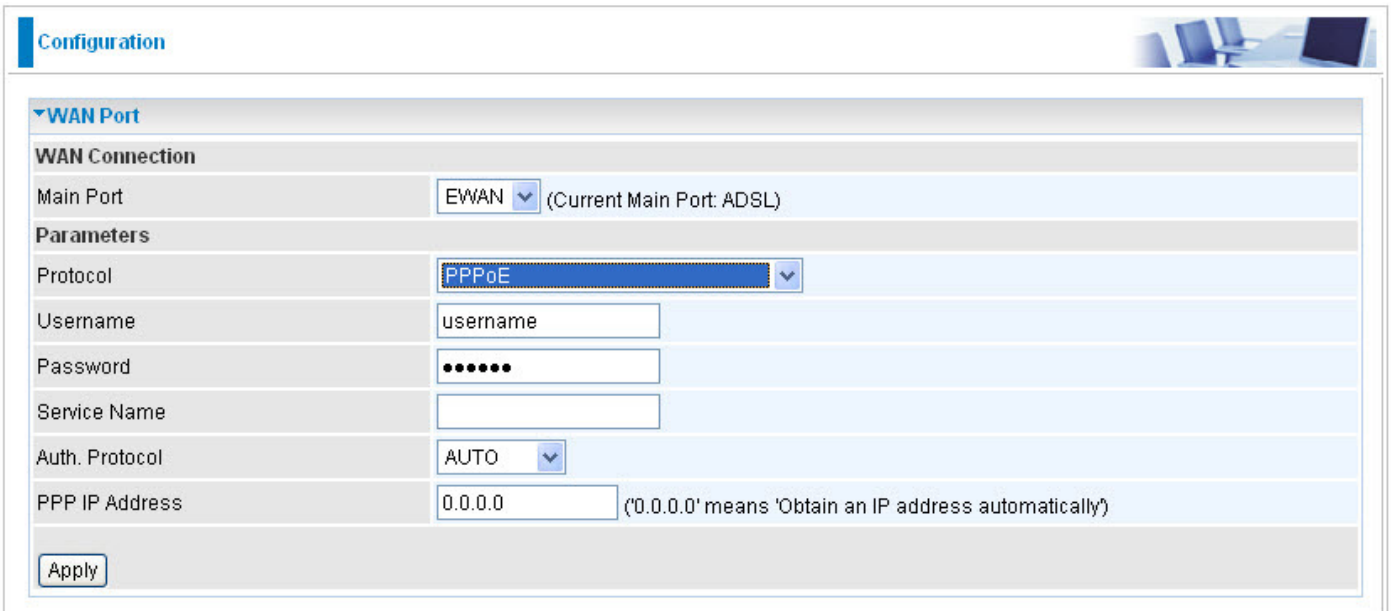
VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

WAN – Main Port (EWAN)

Besides using ADSL to get connected to the Internet, Ethernet port 1 of BEC 7800N can be used as an althernative to connect to Cable Modems, VDSL and fiber optic lines. This alternative not only provides faster connection to the Internet, it also provides users with more flexibility to get online.

PPPoE (EWAN)



Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

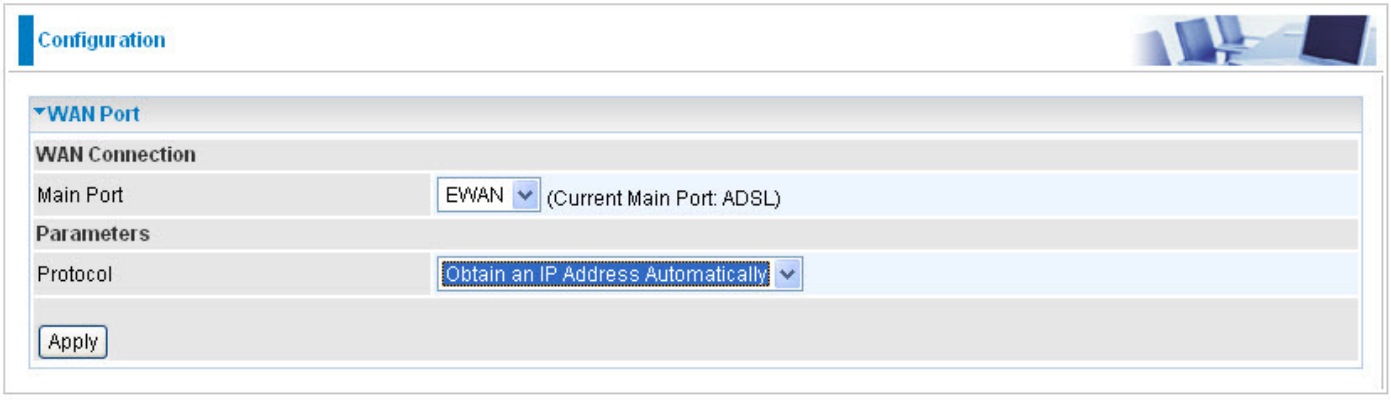
Service Name: This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

Auth. method: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

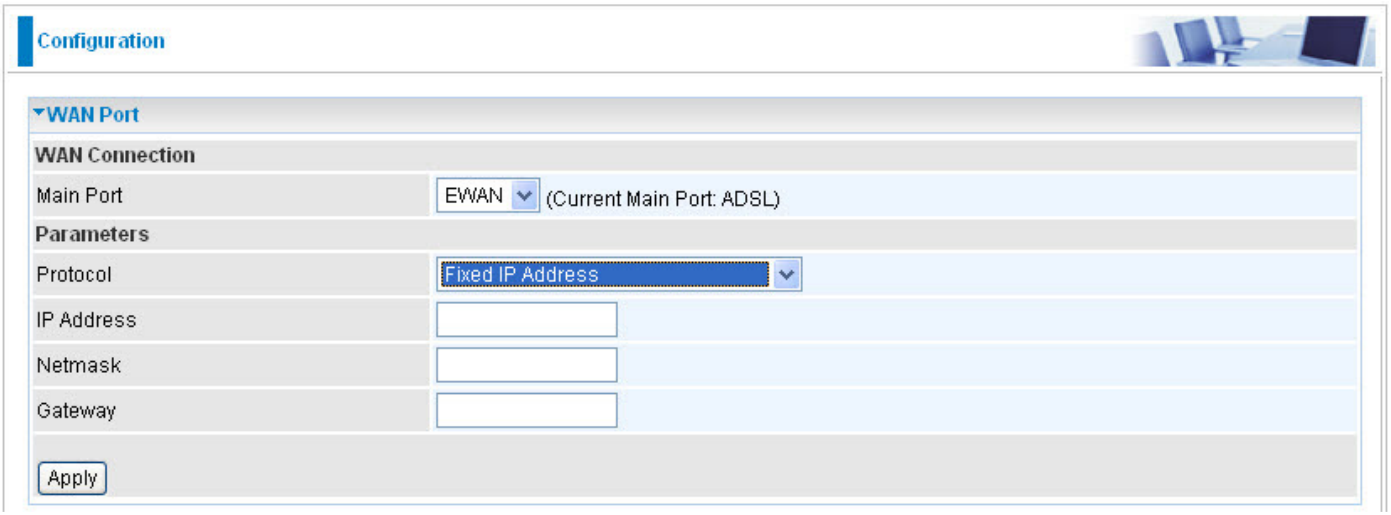
PPP IP Address (0.0.0.0:Auto): Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

Obtain IP Address Automatically (EWAN)

Select this protocol enables the device to automatically retrieve IP address.



Fixed IP Address (EWAN)



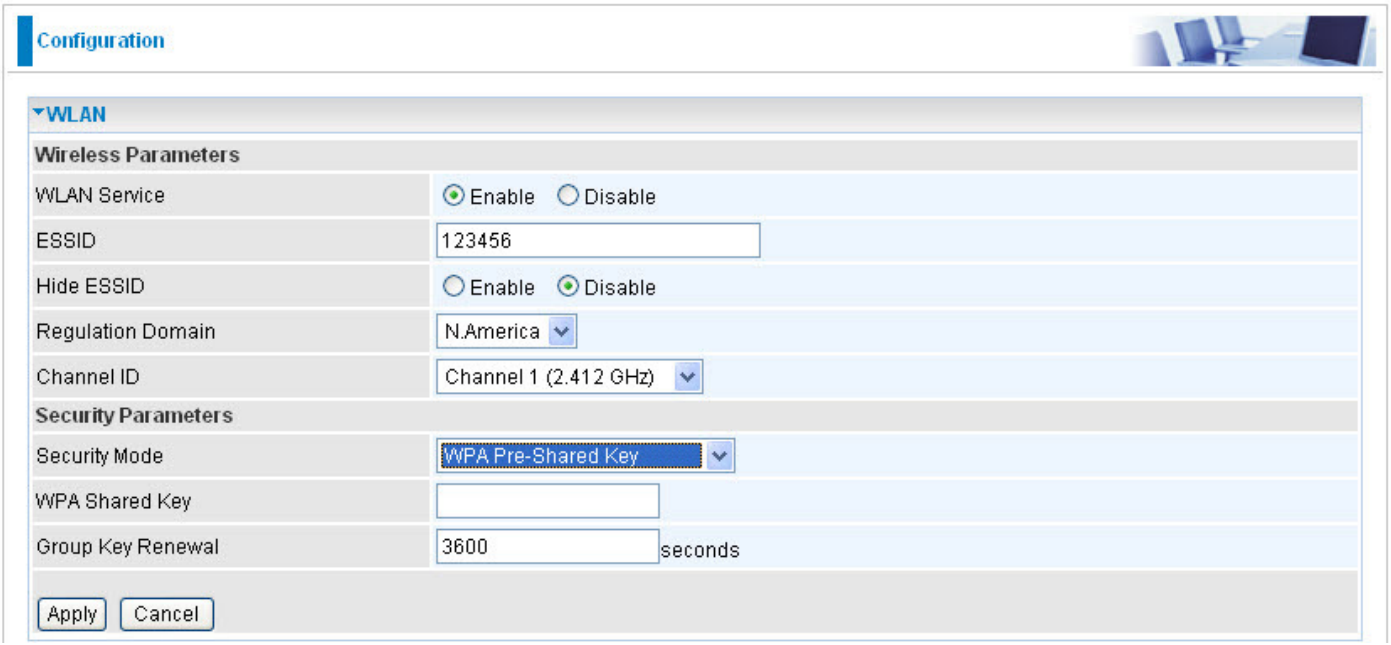
IP Address: Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

Netmask: User can change it to others such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given).

Gateway: Enter the IP address of the default gateway.

WLAN

WPA / WPA2 / WPA/WPA2 Pre-Shared Key



Wireless Parameters

WLAN Service: Default setting is set to Enable. If you do not have any wireless, select Disable.

ESSID: The ESSID is the unique name of a wireless access point (AP) to be distinguished from another. For security purpose, change the default wlan-ap to a unique ID name to the AP already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the ESSID as the device, in order to get connected to your network.

Hide ESSID: This function enables the router to become invisible on the network. Thus, any clients using the wireless setting to search for available or specific router on the network will not be able to discover the router whose Hide ESSID function is set to enabled. The default setting is disabled.

Regulation Domain: There are seven Regulation Domains for you to choose from, including North America (N.America), Europe, France, etc. The Channel ID will be different based on this setting.

Channel ID: Select the wireless connection channel ID that you would like to use.

Note: Wireless performance may degrade if the selected channel ID is already being occupied by other AP(s).

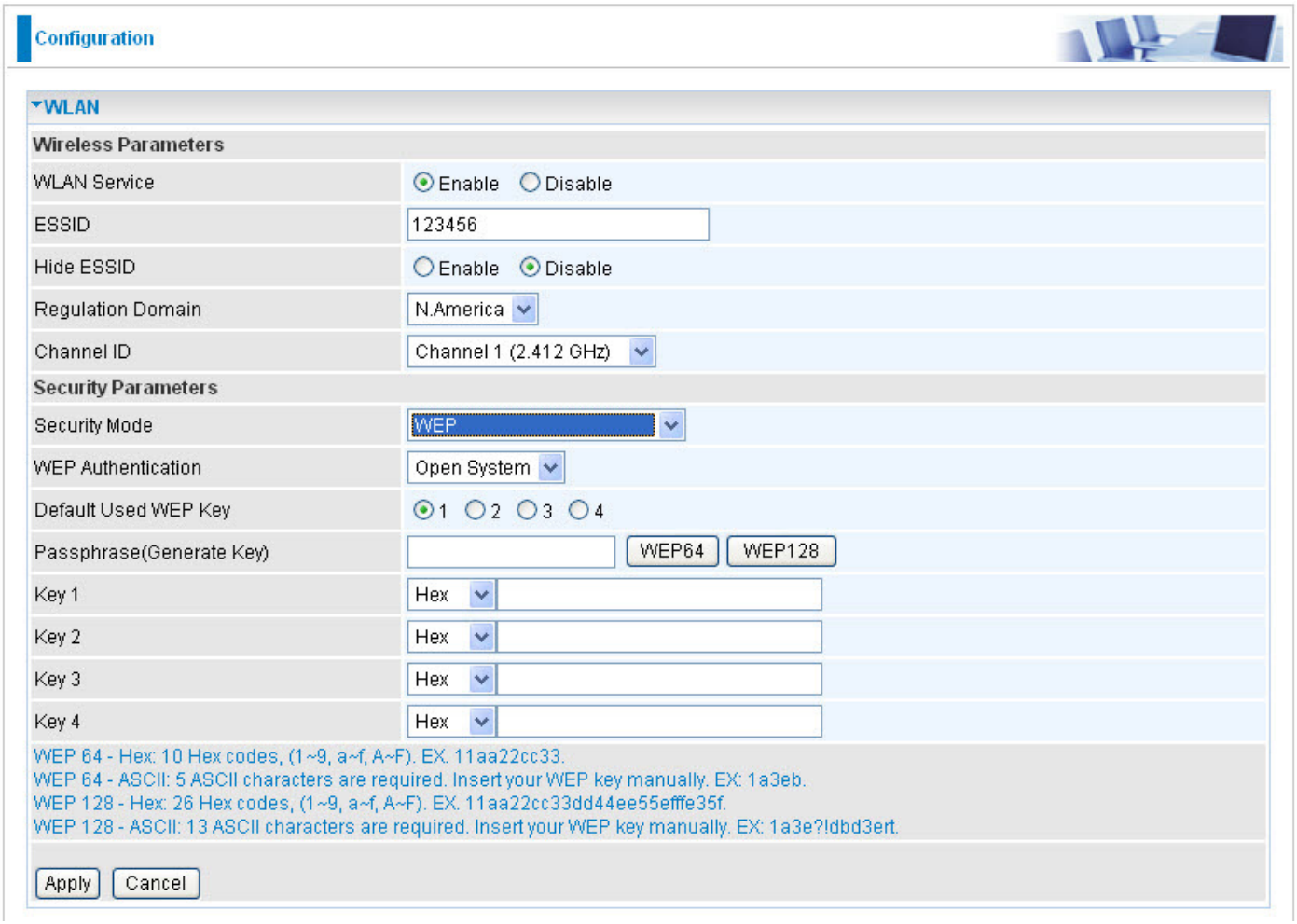
Security Parameters

Security Mode: You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). Default value is 3**600** seconds.

WEP



Parameters

WLAN Service: Default setting is set to Enable. If you do not have any wireless, select Disable.

ESSID: The ESSID is the unique name of a wireless access point (AP) to be distinguished from another. For security purpose, change the default wlan-ap to a unique ID name to the AP already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the ESSID as the device, in order to get connected to your network.

Hide ESSID: This function enables the router to become invisible on the network. Thus, any clients using the wireless setting to search for available or specific router on the network will not be able to discover the router whose Hide ESSID function is set to enabled. The default setting is disabled.

Regulation Domain: There are seven Regulation Domains for you to choose from, including North America (N.America), Europe, France, etc. The Channel ID will be different based on this setting.

Channel ID: Select the wireless connection channel ID that you would like to use.

Note: Wireless performance may degrade if the selected channel ID is already being occupied by other AP(s).

Security Parameters

Security Mode: You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**.

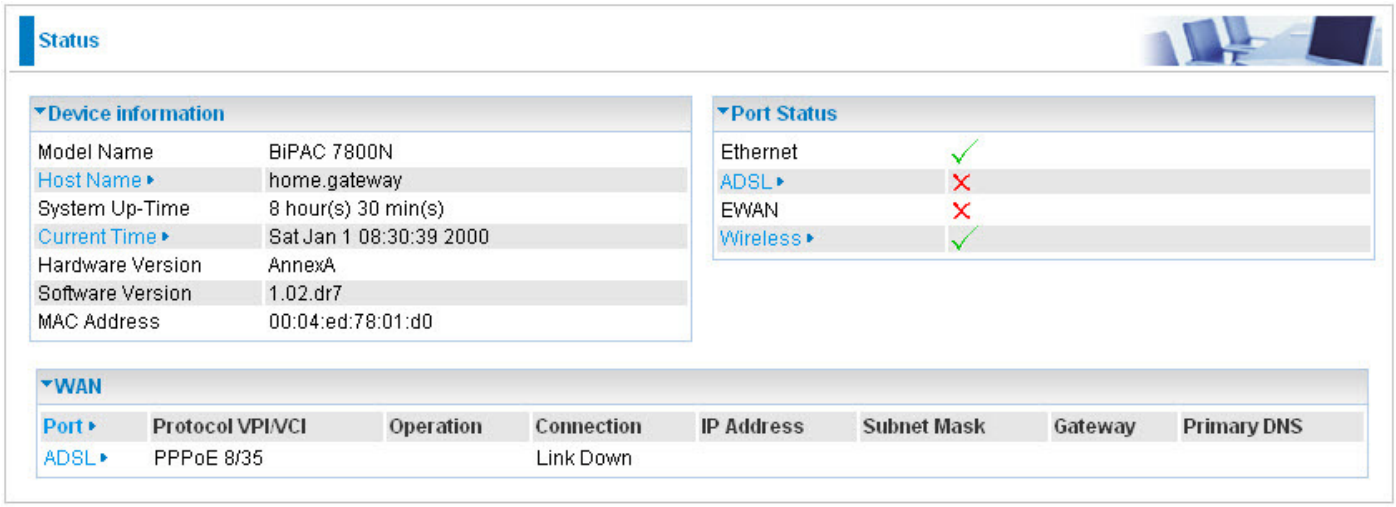
WEP Authentication: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP. If you require high security for transmissions, there are two options to select from: **Open System, Shared key** or **both**.

Default Used WEP Key: Select the encryption key ID; please refer to **Key (1~4)** below.

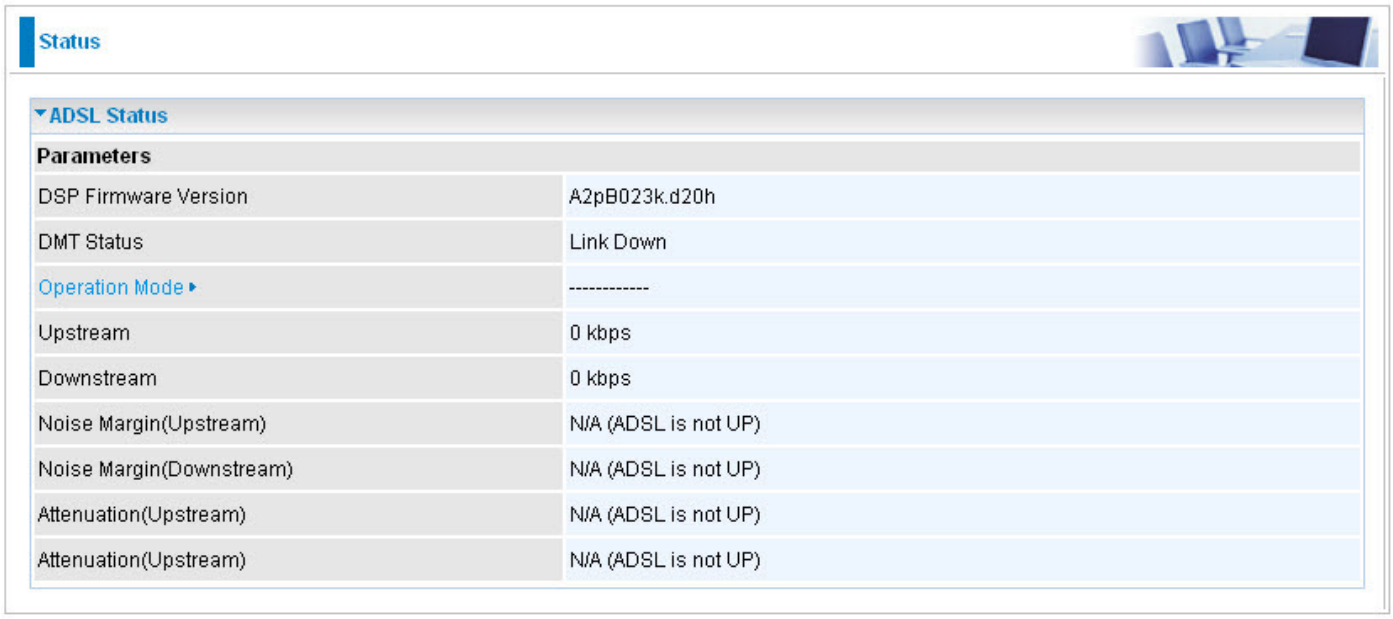
Passphrase: This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128.

Key (1-4): Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX style, 10 and 26 HEX codes are required for WEP64 and WEP128 respectively.

Status (Advanced Mode)



ADSL



DSP Firmware Version: DSP code version.

DMT Status: Current DMT Status.

Operational Mode: Display the ADSL state when the connect mode is set to AUTO.

Upstream: Upstream rate.

Downstream: Downstream rate.

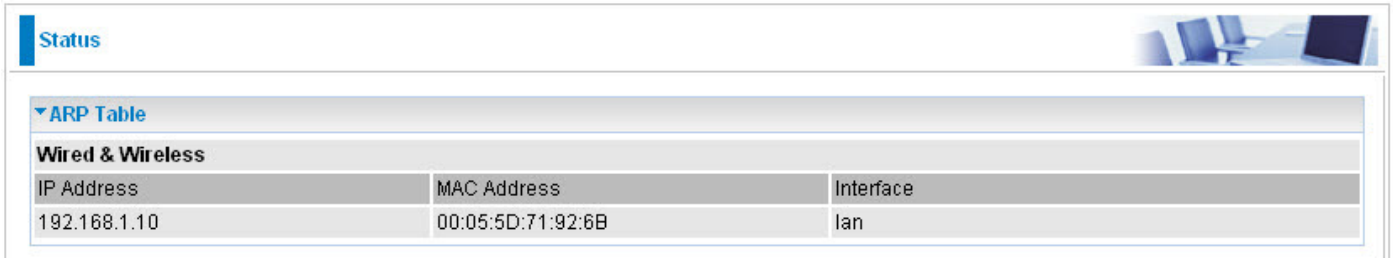
Noise Margin (Upstream): This shows the noise margin for upstream rate.

Noise Margin (Downstream): This shows the noise margin for downstream rate.

Attenuation (Upstream): This is attenuation of signal in upstream.

Attenuation (Downstream): This is attenuation of signal in downstream.

ARP



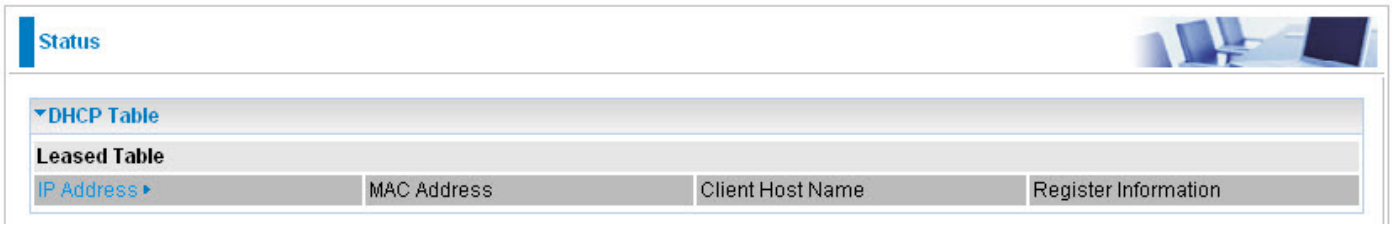
This table shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is useful in determining the MAC address of the network interface of your PCs that use the router's Firewall – MAC Address Filter function. See the Firewall section of this manual for more information on this feature.

IP Address: Shows the IP Address of internal host that join this network as well as the external IP.

MAC Address: The MAC address of internal host.

Interface: The interface name (on the router) that this IP address connects to.

DHCP



IP Address: Click to access the DHCP server configuration page.

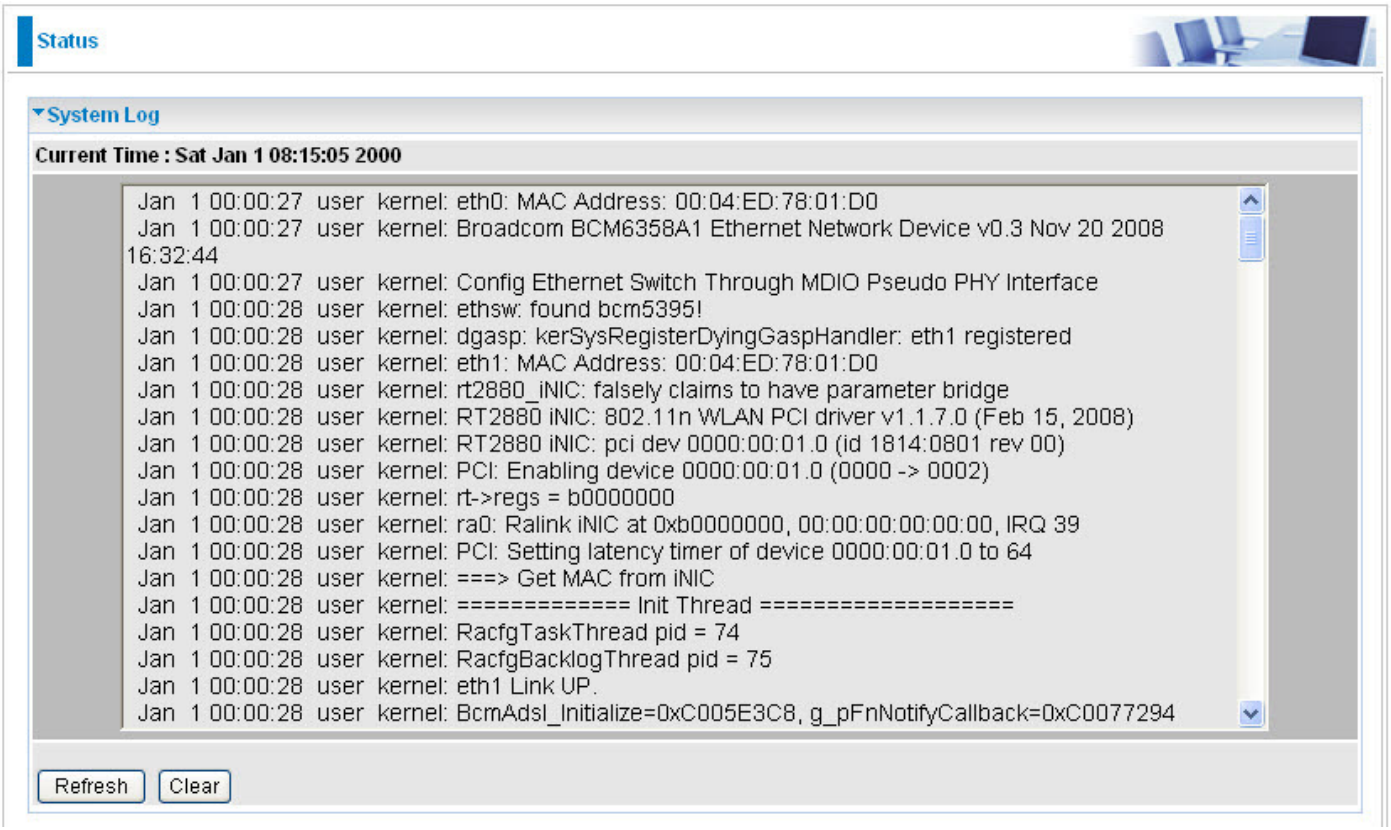
MAC Address: The MAC Address of internal dhcp client host.

Client Host Name: The Host Name of internal dhcp client.

Register Information: Shows the information provided during registration.

System Log

Display all the system logs that have been recorded up to the present time.


Status
System Log
Current Time : Sat Jan 1 08:15:05 2000
Jan 1 00:00:27 user kernel: eth0: MAC Address: 00:04:ED:78:01:D0
Jan 1 00:00:27 user kernel: Broadcom BCM6358A1 Ethernet Network Device v0.3 Nov 20 2008 16:32:44
Jan 1 00:00:27 user kernel: Config Ethernet Switch Through MDIO Pseudo PHY Interface
Jan 1 00:00:28 user kernel: ethsw: found bcm5395!
Jan 1 00:00:28 user kernel: dgasp: kerSysRegisterDyingGaspHandler: eth1 registered
Jan 1 00:00:28 user kernel: eth1: MAC Address: 00:04:ED:78:01:D0
Jan 1 00:00:28 user kernel: rt2880_iNIC: falsely claims to have parameter bridge
Jan 1 00:00:28 user kernel: RT2880 iNIC: 802.11n WLAN PCI driver v1.1.7.0 (Feb 15, 2008)
Jan 1 00:00:28 user kernel: RT2880 iNIC: pci dev 0000:00:01.0 (id 1814:0801 rev 00)
Jan 1 00:00:28 user kernel: PCI: Enabling device 0000:00:01.0 (0000 -> 0002)
Jan 1 00:00:28 user kernel: rt->regs = b0000000
Jan 1 00:00:28 user kernel: ra0: Ralink iNIC at 0xb0000000, 00:00:00:00:00:00, IRQ 39
Jan 1 00:00:28 user kernel: PCI: Setting latency timer of device 0000:00:01.0 to 64
Jan 1 00:00:28 user kernel: ===> Get MAC from iNIC
Jan 1 00:00:28 user kernel: ============= Init Thread ====================
Jan 1 00:00:28 user kernel: RacfgTaskThread pid = 74
Jan 1 00:00:28 user kernel: RacfgBacklogThread pid = 75
Jan 1 00:00:28 user kernel: eth1 Link UP.
Jan 1 00:00:28 user kernel: BcmAdsl_Initialize=0xC005E3C8, g_pFnNotifyCallback=0xC0077294
Refresh
Clear

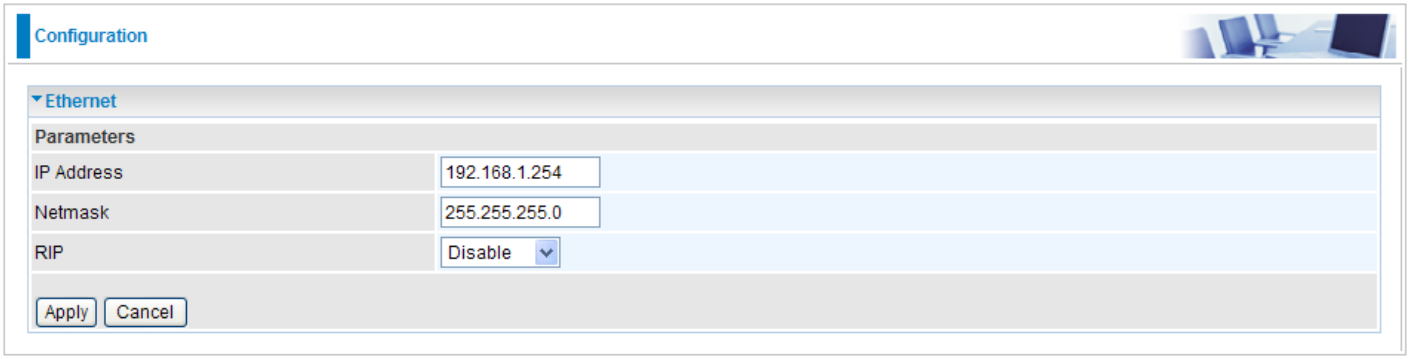
Configuration (Advanced Mode)

LAN

A Local Area Network (LAN) is a shared communication system network where many computers are connected. This type of network is area defined and is usually limited to a confined region within a building or just within the same storey of a building. There are 3 items within the LAN section: **Ethernet**, **IP Alias**, **Wireless**, **Wireless Security** and **DHCP Server**.

Ethernet

The router supports more than one Ethernet IP addresses in the LAN, and with distinct LAN subnets through which you can access the Internet at the same time. Users usually only have one subnet in their LAN. The default IP address for the router is 192.168.1.254.



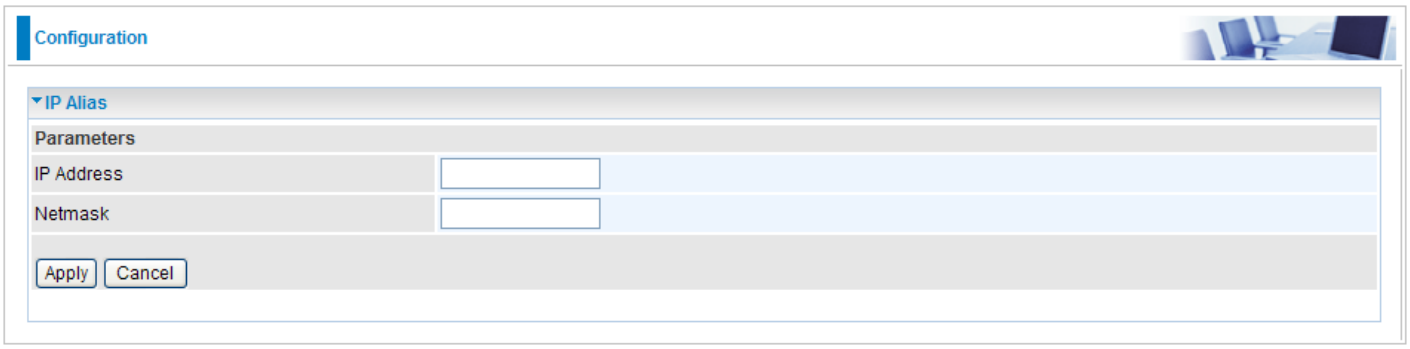
IP Address: The default IP on this router.

Netmask: The default subnet mask on this router. **RIP:**

RIP v1, RIP v2, RIP v1+v2 and RIP v2 Multicast.

IP Alias

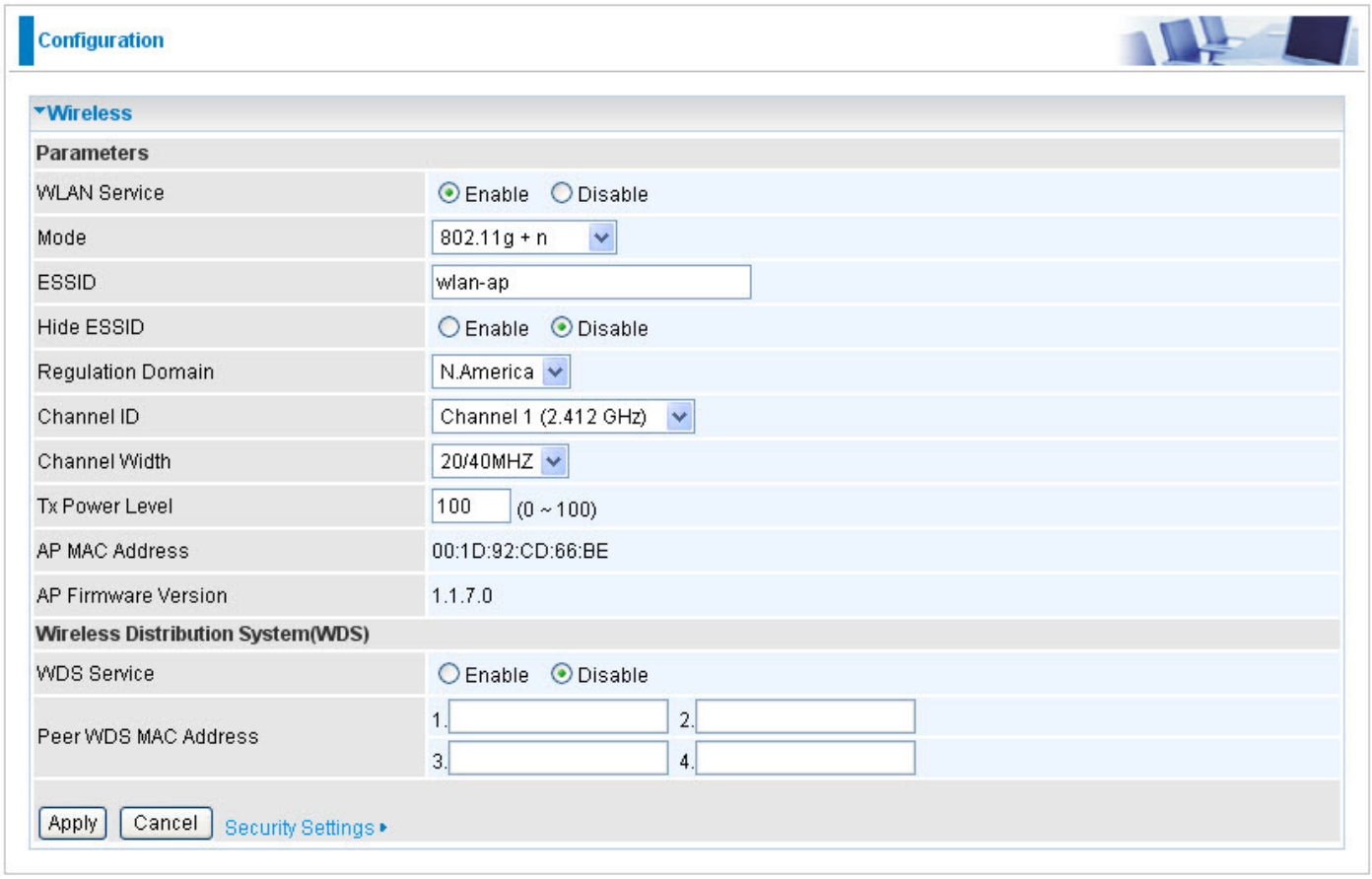
This function allows the addition of more than 1 IP address to the network interface. This further allows user to assign each IP address with specified functions.



IP Address: Enter the IP address to be added to the network.

Netmask: Specify a subnet mask for the IP to be added.

Wireless



Parameters

WLAN Service: Default setting is set to Enable. If you do not have any wireless, select Disable.

Mode: The default setting is 802.11b+g+n (Mixed mode). If you do not know or have both 11g and 11b devices in your network, then keep the default in mixed mode. From the drop-down manual, you can select 802.11g if you have only 11g card. If you have only 11b card, then select 802.11b. And if you have 11n card, you can select 802.11n.

ESSID: The ESSID is the unique name of a wireless access point (AP) to be distinguished from another. For security purpose, change the default wlan-ap to a unique ID name to the AP already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the ESSID as the device, in order to get connected to your network.

Hide ESSID: This function enables the router to become invisible on the network. Thus, any clients using the wireless setting to search for available or specific router on the network will not be able to discover the router whose Hide ESSID function is set to enabled. The default setting is disabled.

Regulation Domain: There are seven Regulation Domains for you to choose from, including North America (N.America), Europe, France, etc. The Channel ID will be different based on this setting.

Channel ID: Select the wireless connection channel ID that you would like to use.

Note: Wireless performance may degrade if select channel ID is already being occupied by other AP(s).

Channel width: Select either 20 MHz or 20/40 MHz for the channel bandwidth. The higher the bandwidth the better the performance will be.

TX PowerLevel: It is a function that enhances the wireless transmitting signal strength. User may adjust this power level from minimum 0 up to maximum 100.

Note: The Power Level maybe different in each access network user premises environment and choose the most suitable level for your network.

AP MAC Address: It is a unique hardware address of the Access Point.

AP Firmware Version: The Access Point firmware version.

Wireless Distribution System (WDS)

It is a wireless access point mode that enables wireless link and communication with other access point. It is easy to be installed simply to define peer's MAC address of the connected AP. WDS takes advantages of cost saving and flexibility which no extra wireless client device is required to bridge between two access points and extending an existing wired or wireless infrastructure network to create a larger network. It can connect up to 4 wireless APs for extending cover range at the same time.

In addition, WDS also enhances its link connection security mode. Key encryption must be the same for both access points and the channel.

WDS Service: The default setting is **Disabled.** Check **Enable** radio button to activate this function.

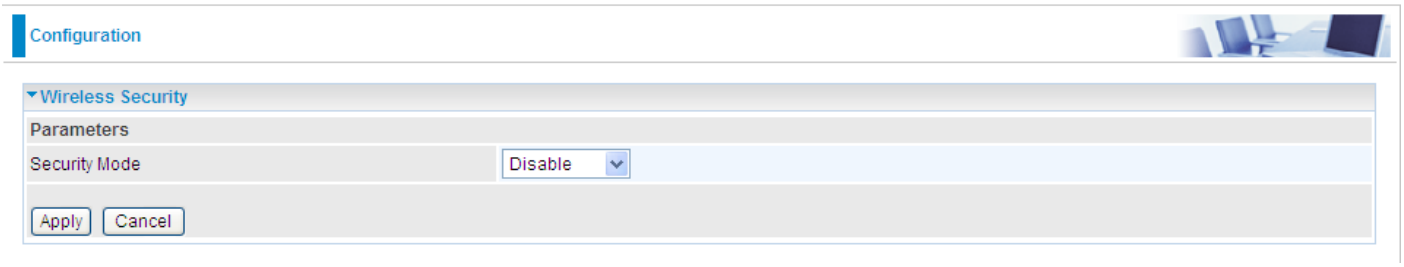
1. **Peer WDS MAC Address:** It is the associated AP's MAC Address. It is important that your peer's AP must include your MAC address in order to acknowledge and communicate with each other.
2. **Peer WDS MAC Address:** It is the second associated AP's MAC Address.
3. **Peer WDS MAC Address:** It is the third associated AP's MAC Address.
4. **Peer WDS MAC Address:** It is the fourth associated AP's MAC Address.

Note: For MAC Address, Semicolon (:) must be included.

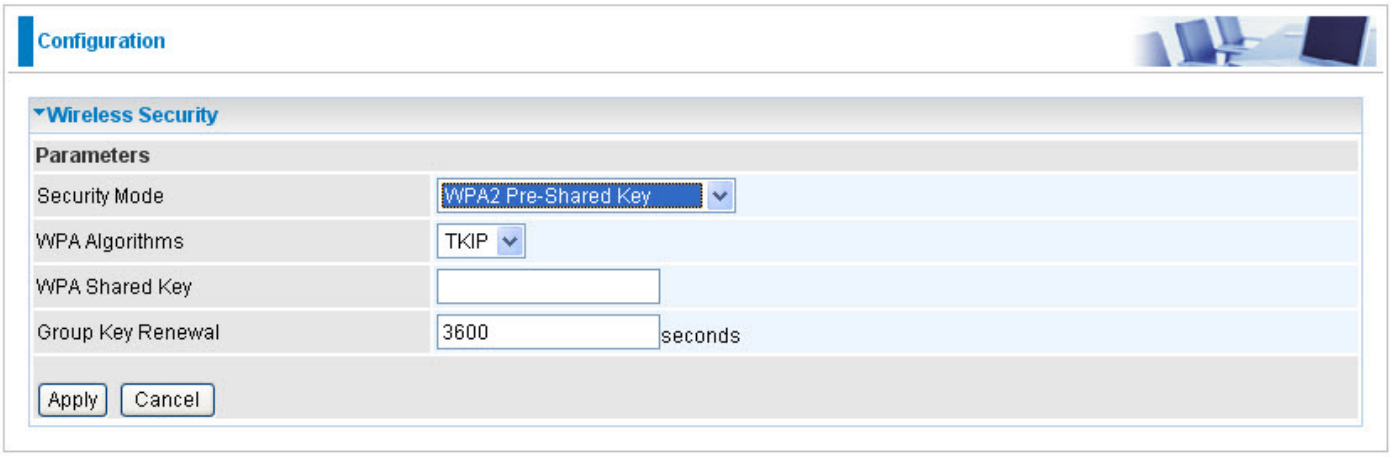
Wireless Security

You can disable or enable with WPA or WEP for protecting wireless network.

The default mode of wireless security is disabled.



WPA / WPA2 / WPA/WPA2 Pre-Shared Key



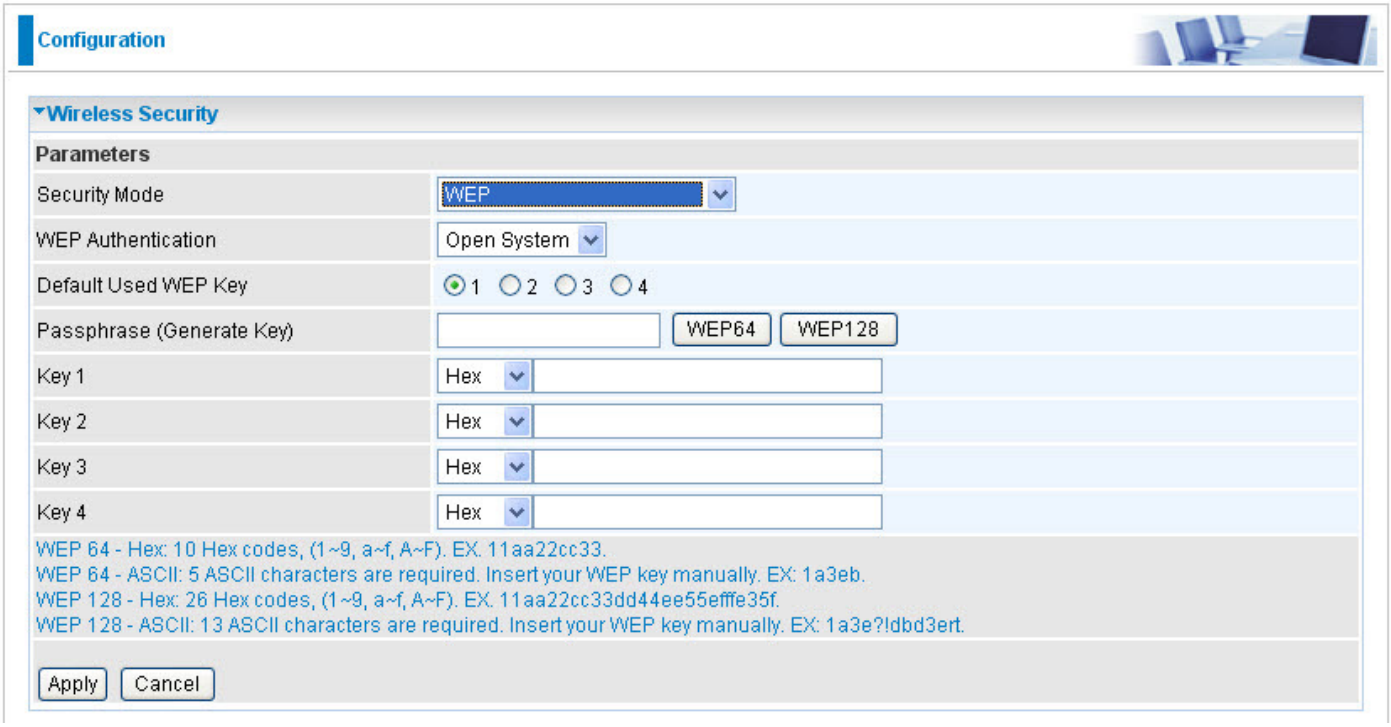
Security Mode: You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**.

WPA Algorithms: There are 3 types of the WPA-PSK, WPA-PSK, WPA2-PSK & WPA/WPA2-PSK. The WPA-PSK adapts the TKIP (Temporal Key Integrity Protocol) encrypted algorithms, which incorporates Message Integrity Code (MIC) to provide protection against hackers. The WPA2-PSK adapts CCMP (Cipher Block Chaining Message Authentication Code Protocol) of the AES (Advanced Encryption Security) algorithms.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). Default value is 3**600** seconds.

WEP



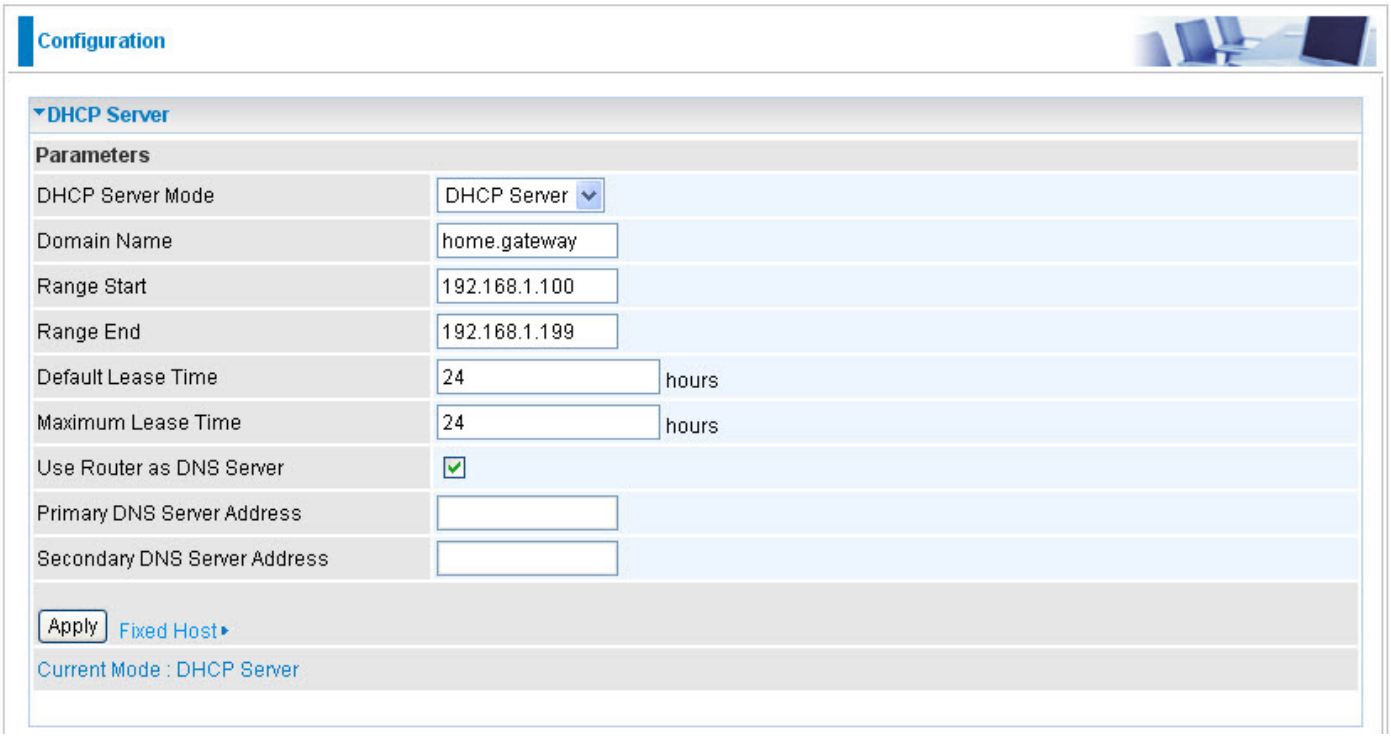
WEP Authentication: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP. If you require high security for transmissions, there are two options to select from: **Open System, Shared key** or **both**.

Default Used WEP Key: Select the encryption key ID; please refer to **Key (1~4)** below.

Passphrase: This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128.

Key (1-4): Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX style, 10 and 26 HEX codes are required for WEP64 and WEP128 respectively.

DHCP Server



DHCP allows networked devices to obtain information on the parameter of IP, Netmask, Gateway as well as DNS through the Ethernet Address of the device. If you check the DHCP Relay you must enter the IP address of the DHCP server that assigns an IP address to the DHCP client in the LAN. Use this function only if advised to do so by your network administrator or ISP. Click Apply to enable this function.

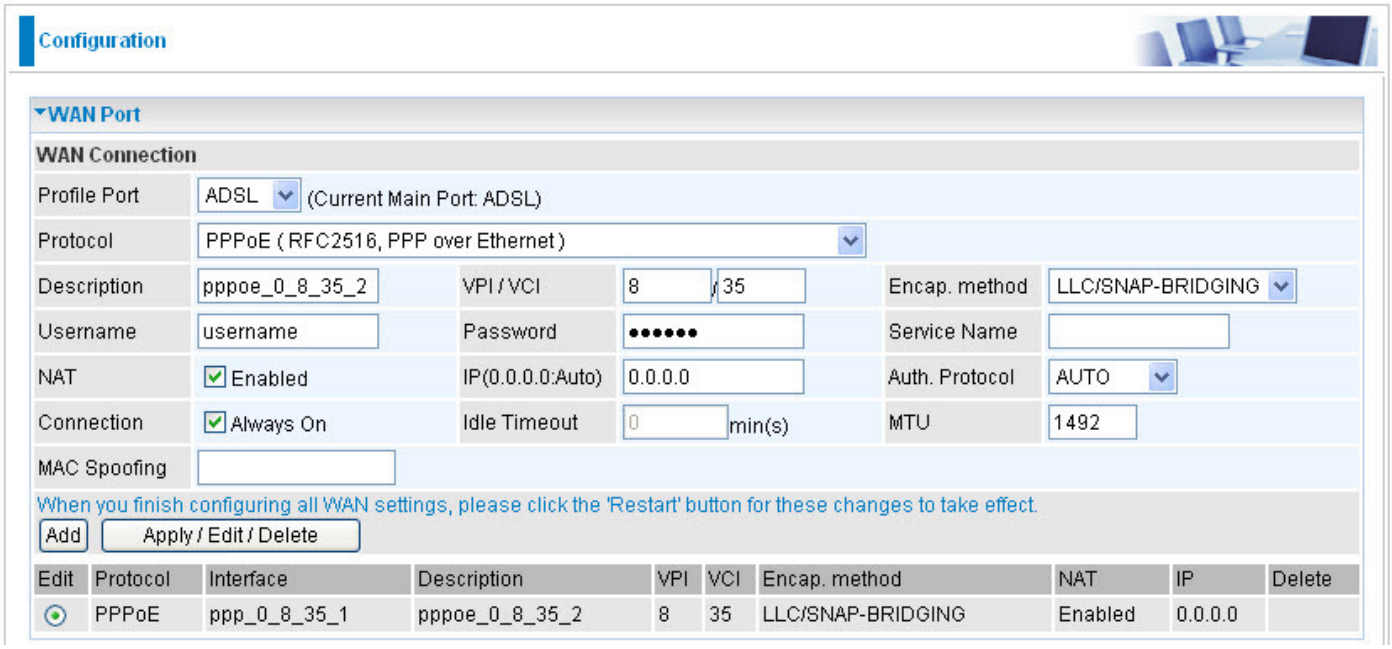
WAN

A WAN (Wide Area Network) is a computer network that covers a broad geographical area (eg. Internet) that is used to connect LAN and other types of network systems. There are two items within the WAN section: **WAN Profile** and **ADSL Mode**.

WAN Profile (ADSL)

PPPoE Connection (ADSL)

PPPoE (PPP over Ethernet) provides access control in a manner similar to dial-up services using PPP.



Description: A given name for the connection.

VPI/VCI: Enter the information provided by your ISP.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing a single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled.

IP (0.0.0.0:Auto): Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

Auth. Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

Connection: Click on **Always on** to establish a PPPoE session during start up and to automatically re-establish the PPPoE session when disconnected by the ISP. You may uncheck the item to disable this function.

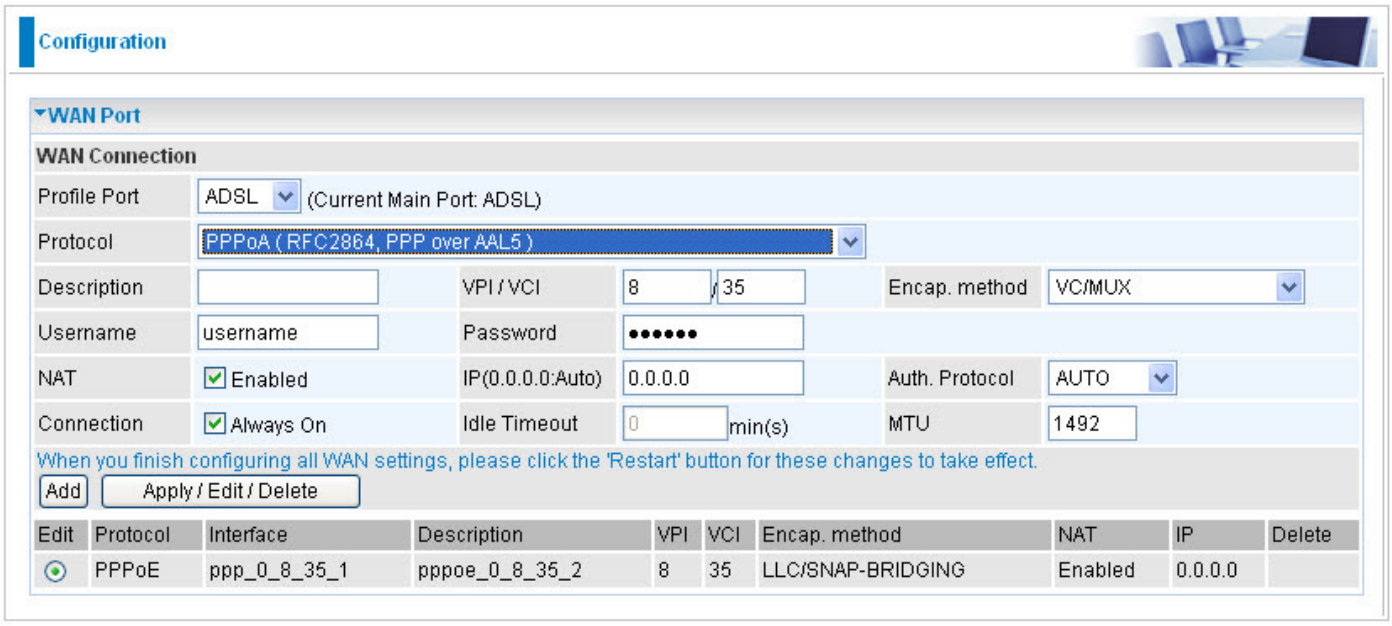
Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.

MTU: Control the maximum Ethernet packet size your PC will send.

MAC Spoofing: This option is required by some service Providers. You must fill the MAC address specified by your service provider when this information is required. The default setting is set to disable.

PPPoA Connection (ADSL)

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). It provides access control and billing functions in a manner similar to dial-up services using PPP.



Description: A given name for the connection.

VPI/VCI: Enter the information provided by your ISP.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing a single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled.

IP (0.0.0.0:Auto): Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

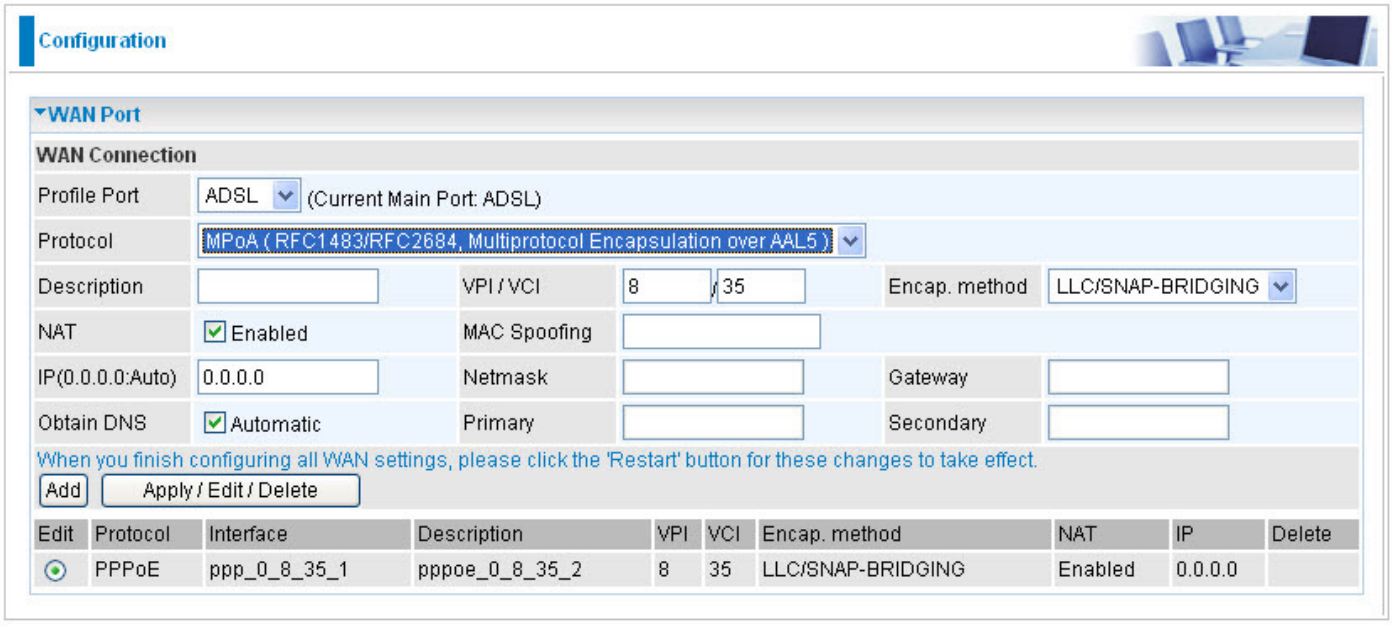
Auth. Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

Connection: Click on **Always on** to establish a PPPoE session during start up and to automatically re-establish the PPPoE session when disconnected by the ISP. You may uncheck the item to disable this function.

Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.

MTU: Control the maximum Ethernet packet size your PC will send.

MPoA Connection (ADSL)



Description: A given name for the connection.

VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account by sharing a single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled.

MAC Spoofing: This option is required by some service Providers. You must fill the MAC address specified by your service provider when this information is required. The default setting is set to disable.

IP Address: Your WAN IP address. If the IP is set to 0.0.0.0 (auto IP detect), both netmask and gateway can be left blank.

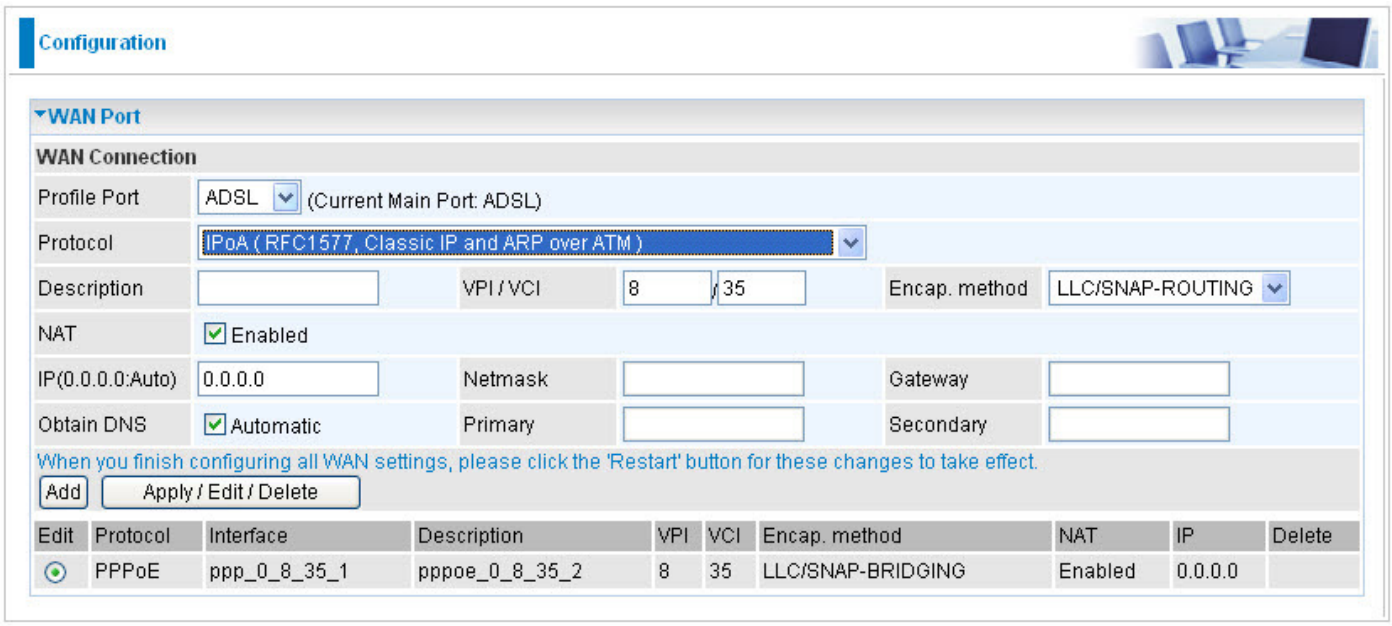
Netmask: User can change it to other such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given)

Gateway: Enter the IP address of the default gateway.

Obtain DNS Automatically: Select this check box to activate DNS.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the netmask.

IPoA Connections (ADSL)



Description: A given name for the connection.

VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account by sharing a single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled.

IP Address: Your WAN IP address. If the IP is set to 0.0.0.0 (auto IP detect), both netmask and gateway can be left blank.

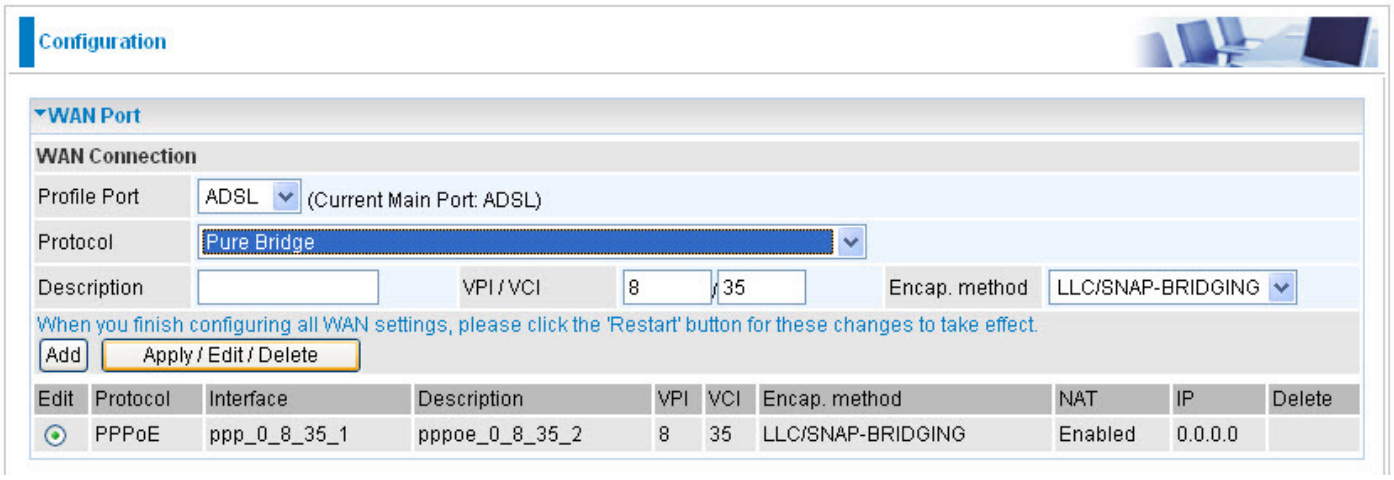
Netmask: User can change it to other such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given)

Gateway: Enter the IP address of the default gateway.

Obtain DNS Automatically: Select this check box to activate DNS.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the netmask.

Pure Bridge Connections (ADSL)



Description: A given name for the connection.

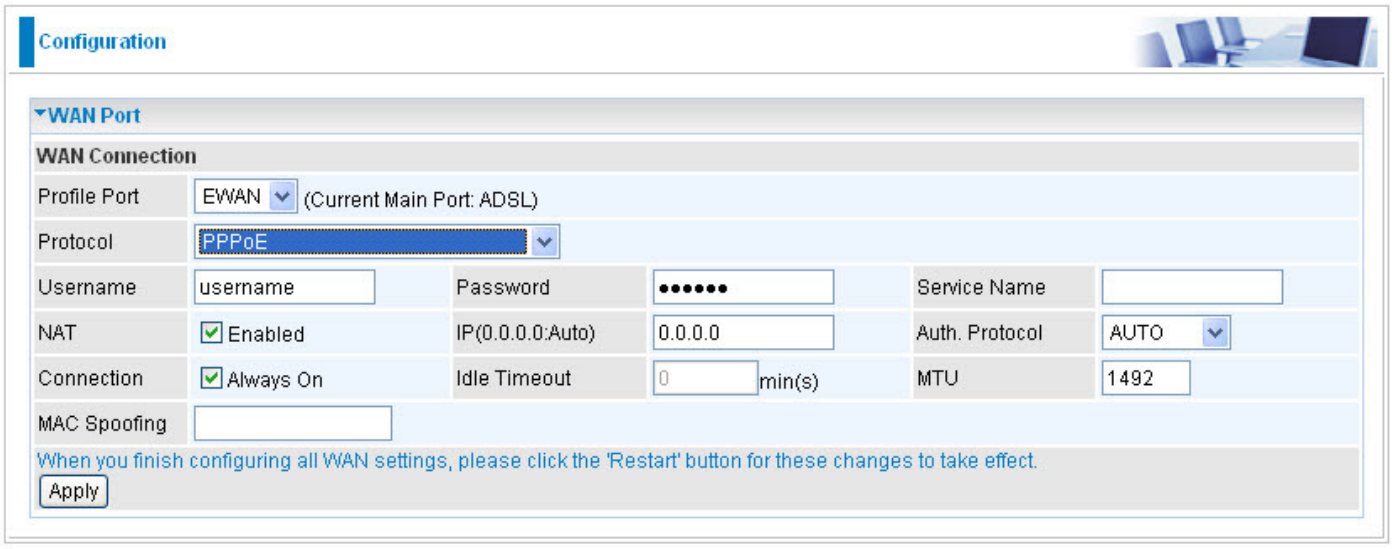
VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

WAN Profile – Main Port (EWAN)

Besides using ADSL to connect to the Internet, BEC 7800 Ethernet port 1 is also an alternative to connect to Cable Modems, VDSL and fiber optic lines. This alternative provides users with faster connection & flexibility to connect to the Internet.

PPPoE (EWAN)



Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled.

IP (0.0.0.0:Auto): Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

Auth. Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

Connection: Click on **Always on** to establish a PPPoE session during start up and to automatically re-establish the PPPoE session when disconnected by the ISP. You may uncheck the item to disable this function.

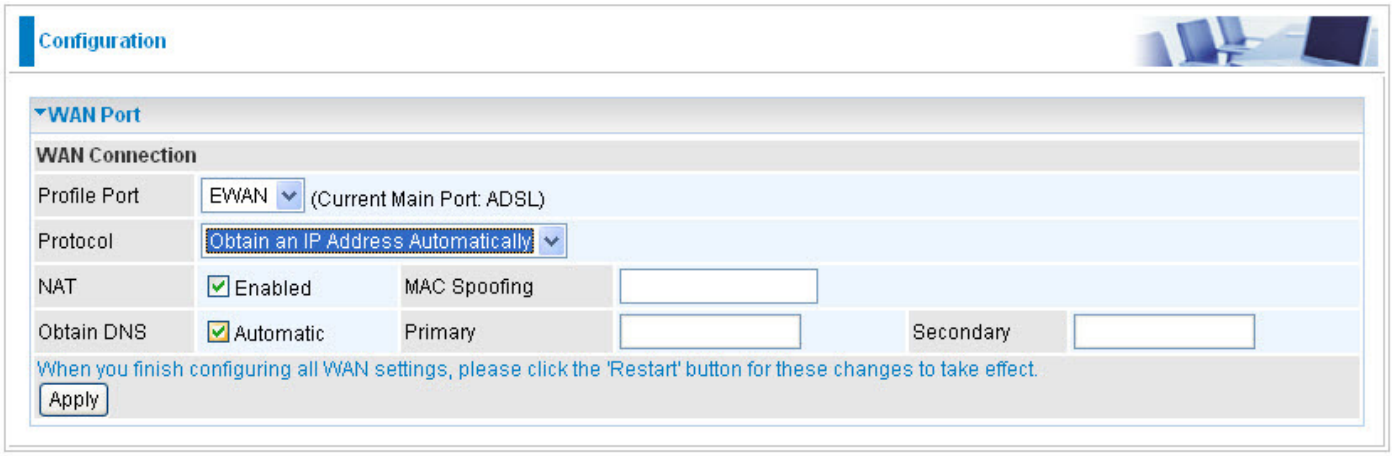
Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.

MTU: Control the maximum Ethernet packet size your PC will send.

MAC Spoofing: This option is required by some service Providers. You must fill the MAC address

specified by your service provider when this information is required. The default setting is set to disable.

Obtain an IP Address Automatically



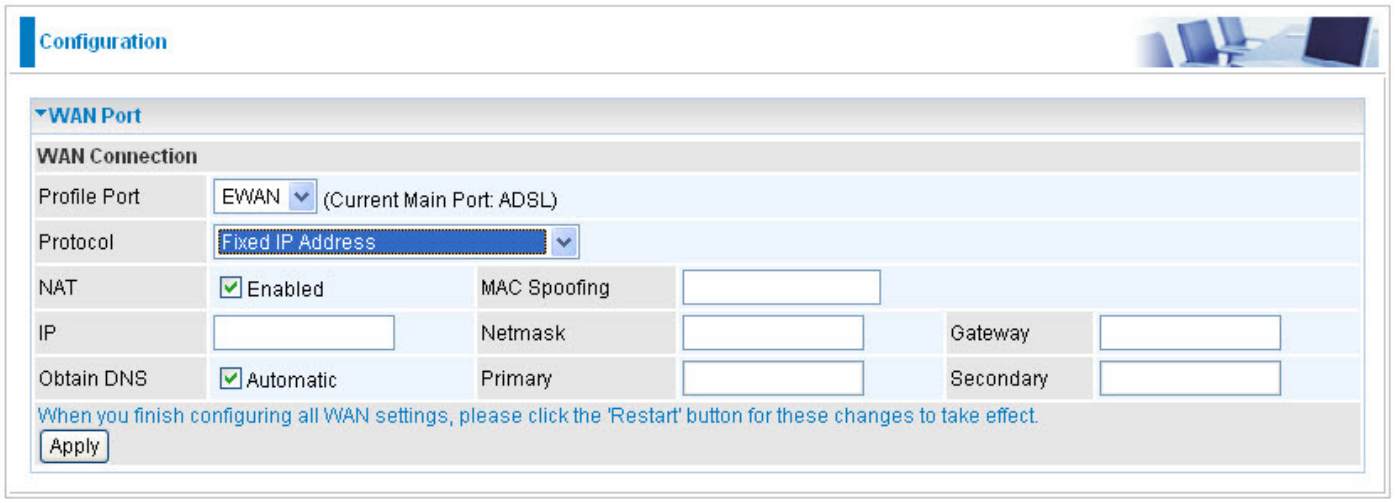
NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled.

MAC Spoofing: This option is required by some service Providers. You must fill the MAC address specified by your service provider when this information is required. The default setting is set to disable.

Obtain DNS: Select this check box to activate DNS.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the netmask.

Fixed IP Address



NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled.

MAC Spoofing: This option is required by some service Providers. You must fill the MAC address specified by your service provider when this information is required. The default setting is set to disable.

IP Address: Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

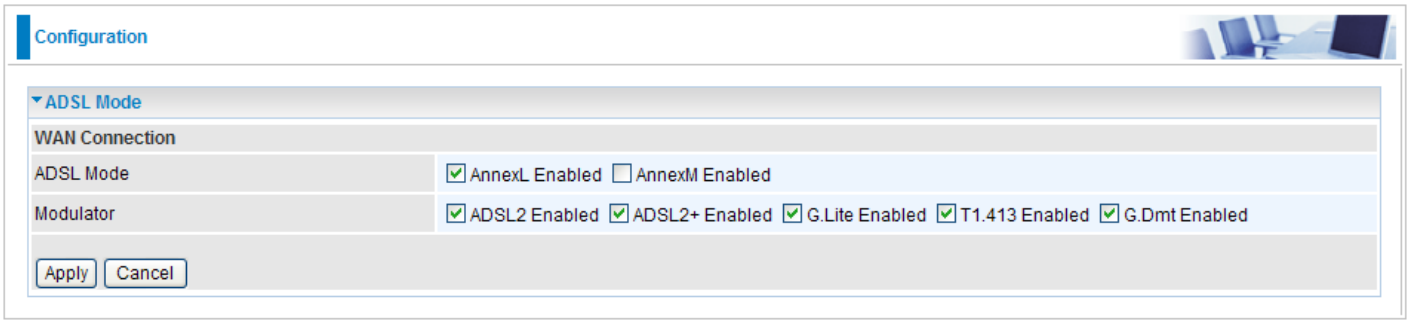
Netmask: User can change it to others such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given)

Gateway: Enter the IP address of the default gateway.

Obtain DNS: Select this check box to activate DNS.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the netmask.

ADSL Mode



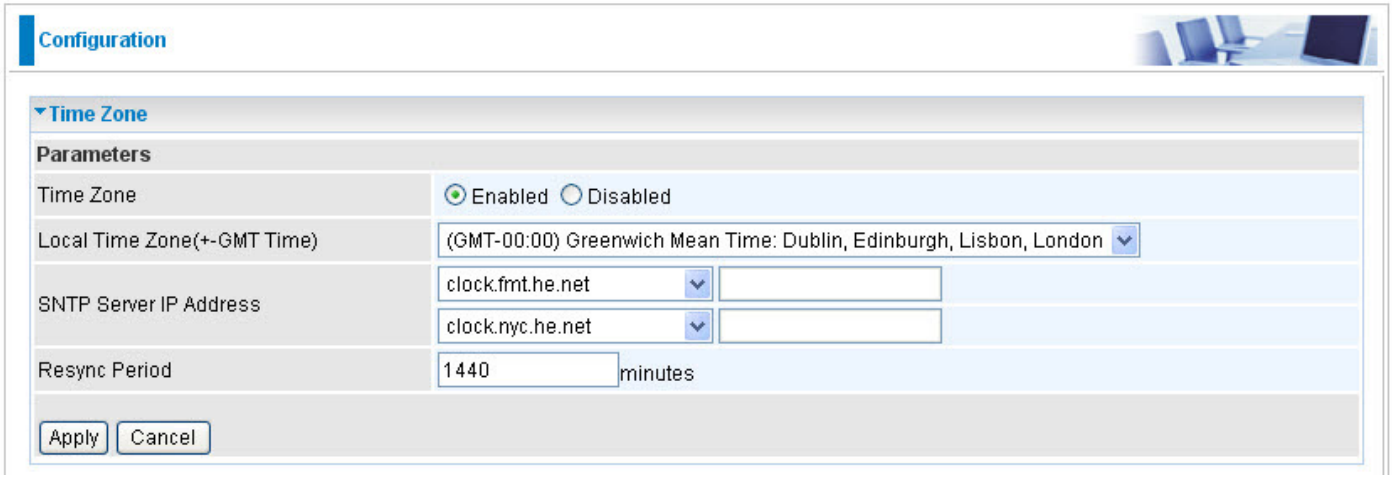
ADSL Mode: There are 2 modes “Annex L” and ”Annex M” that user can select for this connection.

Modulator: There are 5 modes “ADSL2”, ”ADSL2+”, “G.Lite:”, “T1.413” and “G.DMT” that user can select for this connection.

System

There are five items within the System section: **Time Zone, Firmware Upgrade, Backup/ Restore, Restart and User Management.**

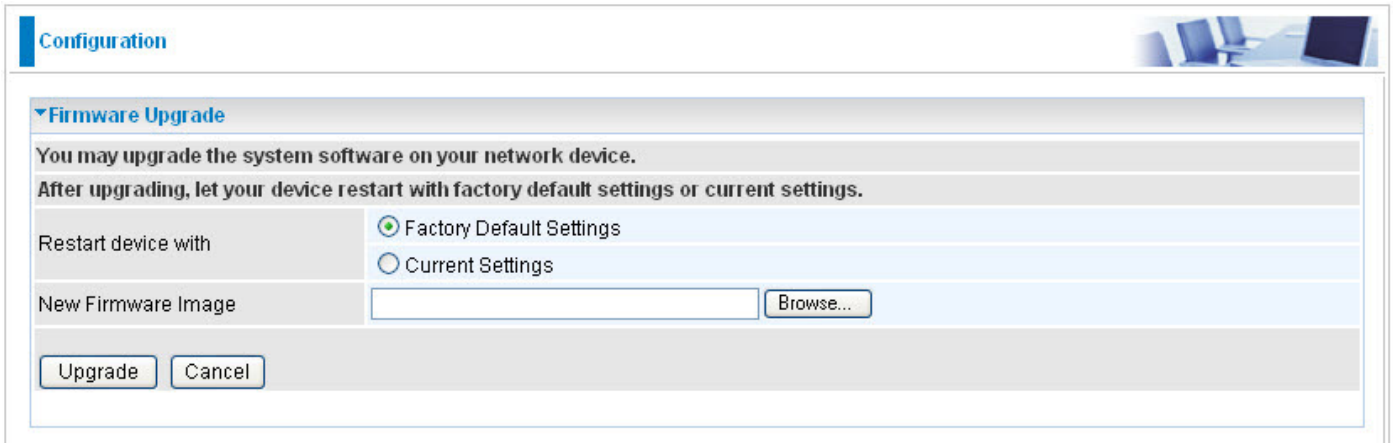
Time Zone



The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the most current time from an SNTP server outside your network. Choose your local time zone from the drop down menu. To apply the selected local time zone, click Enable and click the Apply button. After a successful connection to the Internet, the router will retrieve the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP server other than those in the drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an SNTP server for you to use.

Resync Period (in minutes) is the periodic interval the router will wait before it re-synchronizes the router's time with that of the specified SNTP server. In order to avoid unnecessarily increasing the load on your specified SNTP server you should keep the poll interval as high as possible – at the absolute minimum every few hours or even days. The default value is set at 1440 minutes.

Firmware Upgrade



Your router's "firmware" is the software that allows it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software that runs in your router. Thus, by upgrading the newly improved version of the firmware allows you the advantage to use newly integrated features.

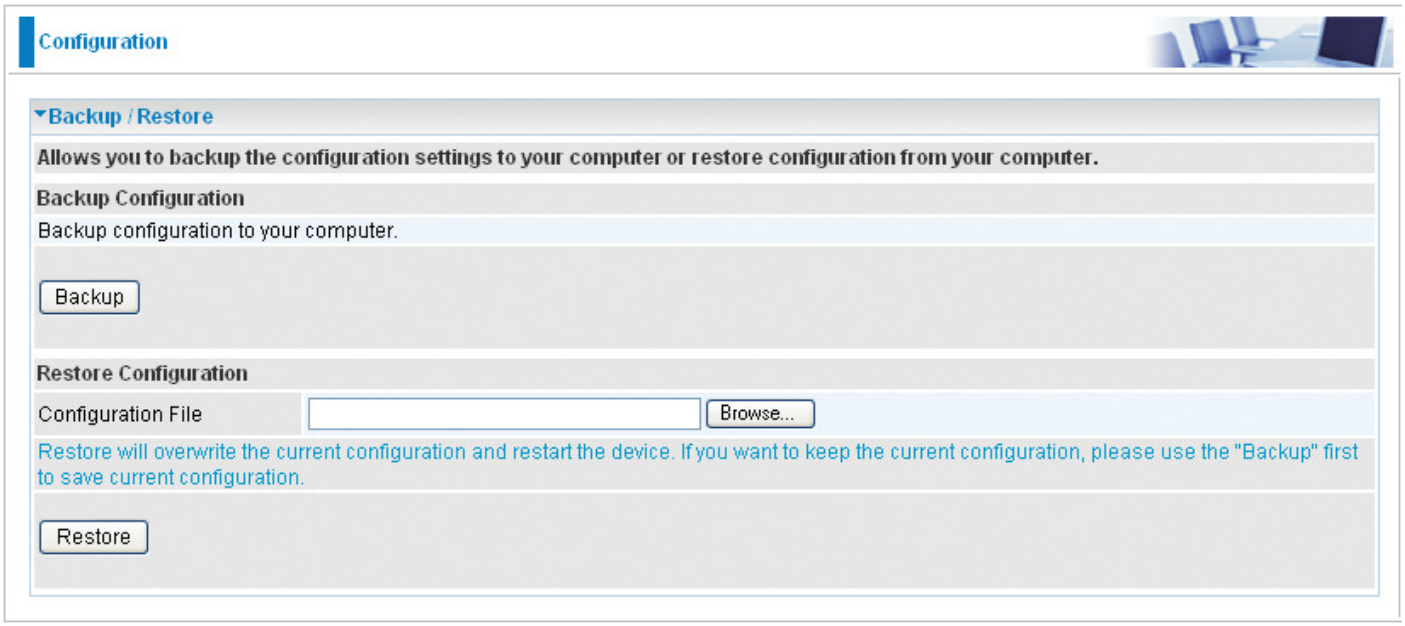
Factory Default Settings: If select this setting, the device will reboot to restore the parameters of all its applications to its default values.

Current Settings: If select this setting, the device will reboot and retain the customized settings of all applications.

Click on Browse to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click Upgrade to update the firmware to your router.

DO NOT power down the router or interrupt the firmware upgrading while it is still in process. Improper operation could damage the router.

Backup / Restore


Configuration
Backup / Restore
Allows you to backup the configuration settings to your computer or restore configuration from your computer.
Backup Configuration
Backup configuration to your computer.
Backup
Restore Configuration
Configuration File
Browse...
Restore will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use the "Backup" first to save current configuration.
Restore

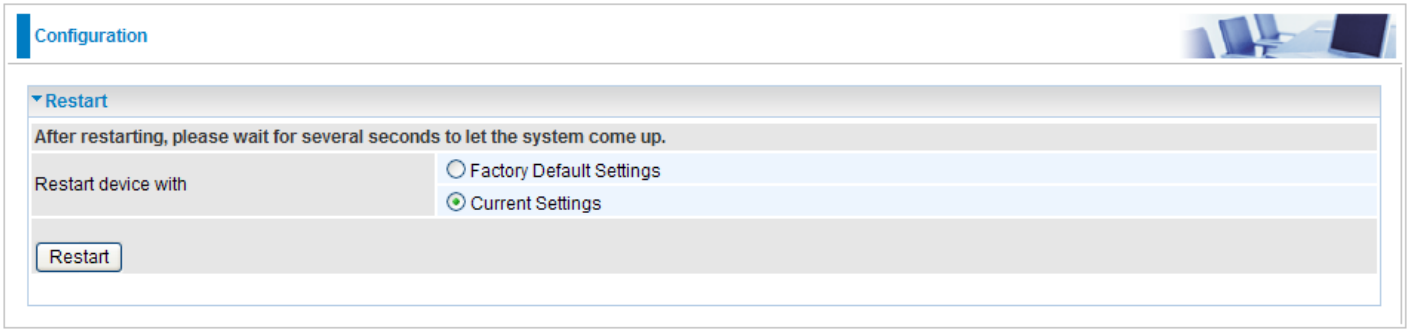
These functions allow you to save a backup of the current configuration of your router to a defined location on your PC, or to restore a previously saved configuration. This is useful if you wish to experiment with different settings, knowing that you have a backup in hand in case any mistakes occur. It is advisable that you backup your router configuration before making any changes to your router configuration.

Press Backup Settings to select where on your local PC you want to store your setting file. You may also want to change the name of the file when saving if you wish to keep multiple backups.

Press Browse… to select a file from your PC to restore. You should only restore your router setting that has been generated by the Backup function which is created with the current version of the router firmware. Settings files saved to your PC should not be manually edited in any way.

Select the settings files you wish to use, and press Update Settings to load the setting into the router.

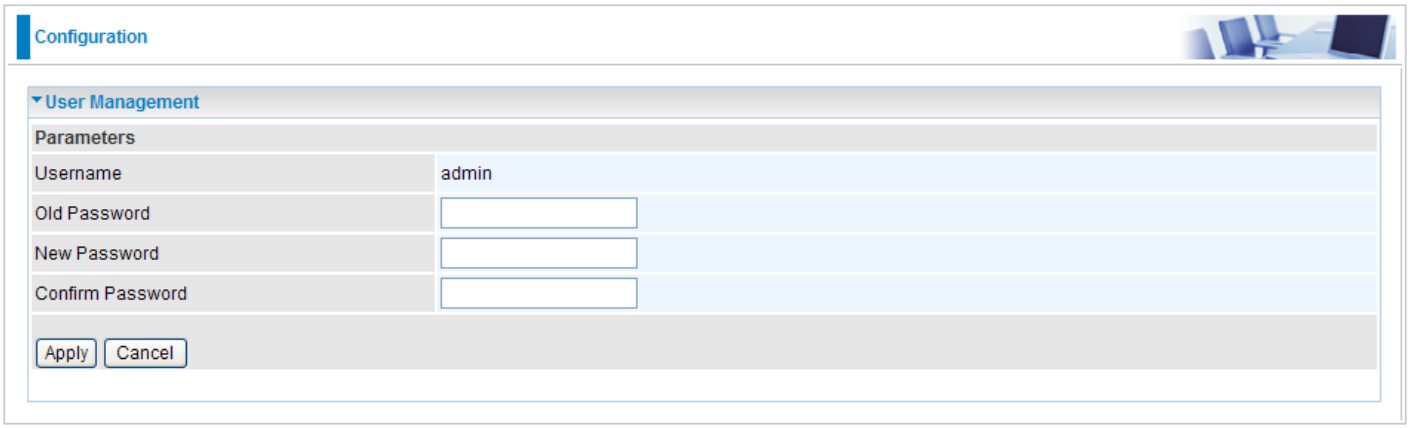
Restart



There are 2 options for you to choose from before restarting the your 7800N device. You can either choose to restart your device to restore it to the Factory Default Settings or to restart the device with your current settings applied. Restarting your device to Factory Default Setting will be useful especially after you have accidentally changed your settings that may result in undesirable outcome.

After selecting the type of setting you want the device to restart with, click the Restart button to initiate the process. After restarting, please wait several minutes to let the selected setting applied to the system.

User Management



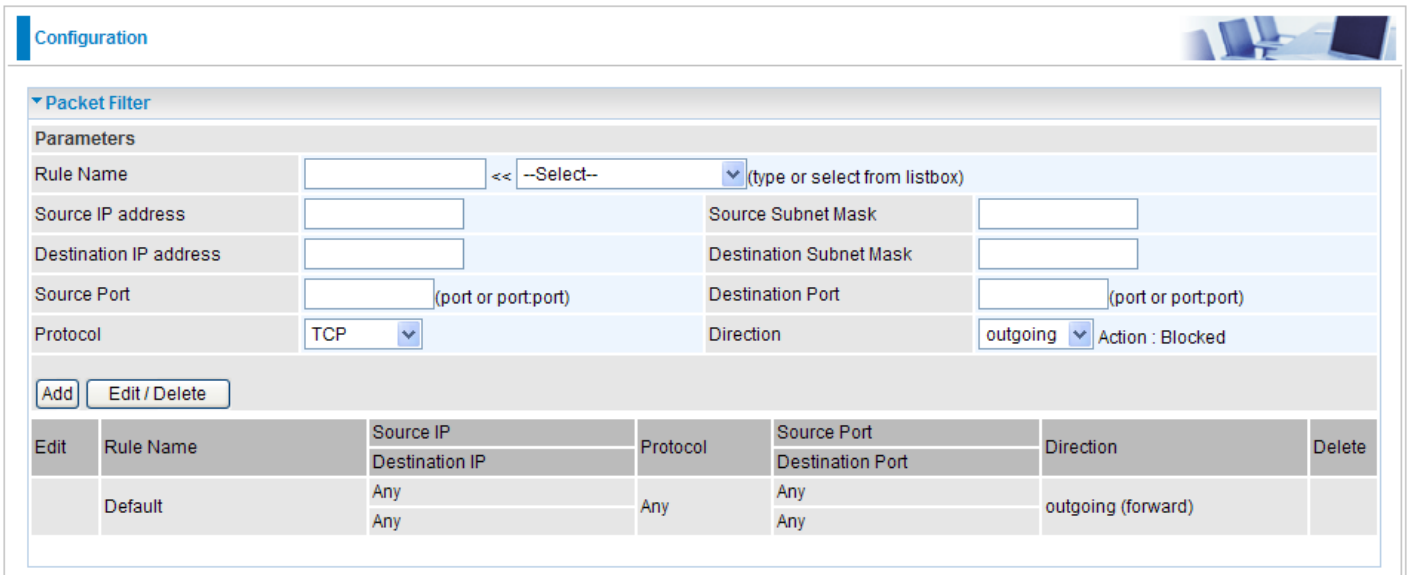
In order to prevent unauthorized access to your router configuration interface, it requires all users to login with a username and password. Therefore only system administrator can access the system. It is highly recommended that you change your password upon receiving your router. The default password is “admin”.

To change your password, simply enter the old password in the Old Password blank. Then enter your new password in the New Password and Confirm Password blanks provided. When this is done, press Apply to save changes.

Firewall

Packet Filter

Packet filtering enables you to configure your router to block specified internal/external users (IP address) from Internet access, or you can disable specific service requests (Port number) to / from the Internet. This configuration program allows you to set up different filter rules for different users based on their IP addresses or their network Port number. The relationship among all filters is “or” operation, which means that the router checks these different filter rules one by one, starting from the first rule. As long as one of the rules is satisfied, the specified action will be taken.



Rule Name: User defined description for entry identification. The maximum name length is 32 characters, and then can choose an application that they want from the listbox.

Source IP address / **Source Subnet Mask:** This is an Address-Filter used to allow or block traffic to/from particular IP address(es). Enter the IP & subnet mask you want to filter. If you leave empty, it means any IP address.

Destination IP address / **Destination Subnet Mask:** This is an Address-Filter used to allow or block traffic to/from particular IP address(es). Enter the IP & subnet mask you want to filter. If you leave empty, it means any IP address.

Source Port: This Port or Port Range defines the ports allowed by the Remote/WAN to connect to the application. Default is set from range 0 ~ 65535. It is recommended that only advance user is to configure this feature.

Destination Port: This is the Port or Port Range that defines the port of the application.

Protocol: Specify the packet type (TCP, UDP, TCP/UDP) that the rule applies to. Select TCP if you wish to search for the connection-based application service on the remote server using the port number. Or select UDP if you want to search for the connectionless application service on the remote server using the port number.

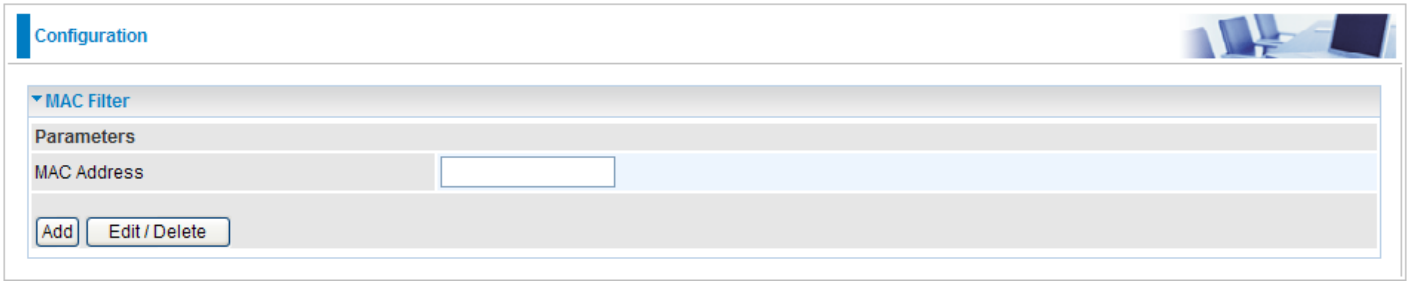
Direction: Determine whether the rule is for outgoing packets or for incoming packets.

Add: Click this button to add a new packet filter rule and the added rule will appear at the bottom table.

Edit: Check the Rule No. you wish to edit, and then click “Edit”.

Delete: Check the Rule No. you wish to delete, and then click “Delete”.

MAC Filter

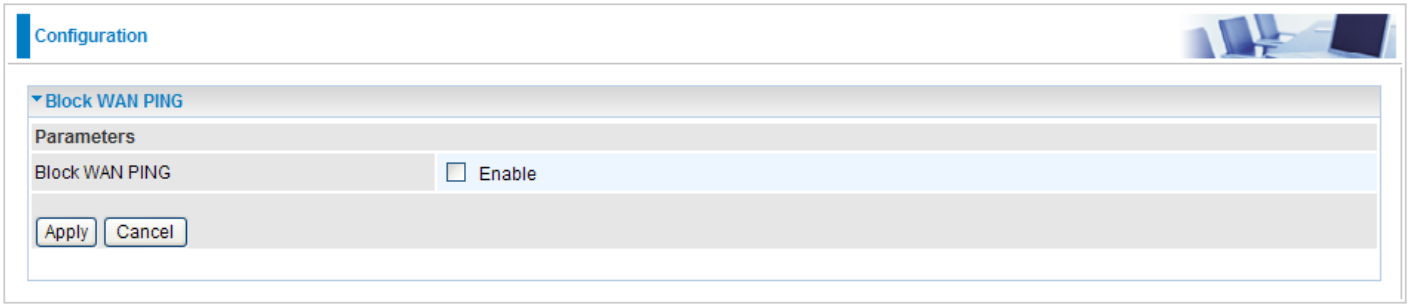


A MAC (Media Access Control) address is the unique network hardware identifier for each PC on your network's interface (i.e. its Network Interface Card or Ethernet card). Using your router's MAC Address Filter function, you can configure the network to block specific machines from accessing your LAN.

To filter a specific MAC address, enter the MAC address in the blank provided then press Add.

The format of MAC address-- could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx

Block WAN Ping



This feature is to be enabled when you want the public WAN IP address on your router not to respond to any ping command.

To activate the Block WAN PING feature, check the Enable box then click the Apply button. This feature is disabled by default.

Virtual Server

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side.

In TCP and UDP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known ports”. Servers follow the well-known port assignments so clients can locate them.

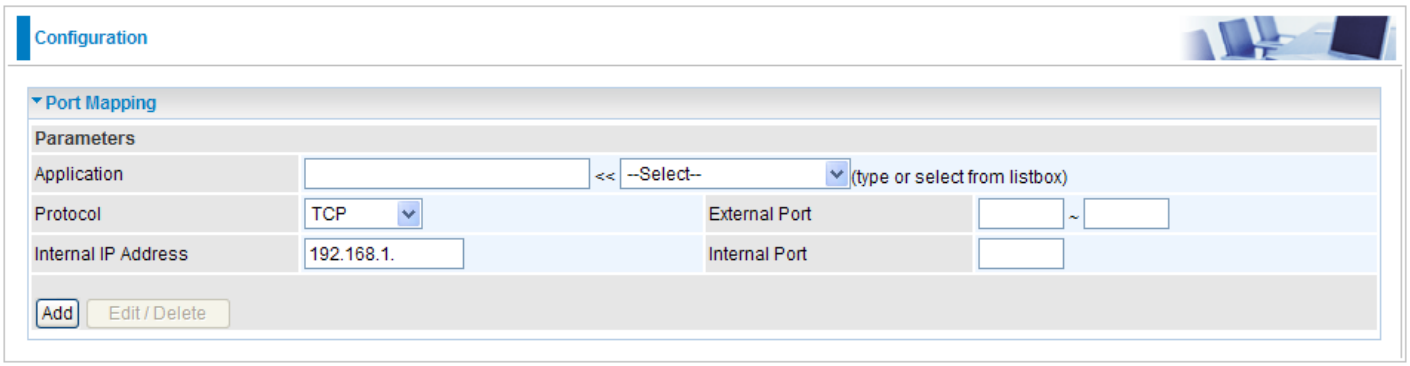
If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You also need to use port forwarding if you wish to host an online game server.

Examples of well-known and registered port numbers are shown below, for further information, please see IANA’s website at: **http://www.iana.org/assignments/port-numbers**

Well-known and Registered Ports

Port Number	Protocol	Description
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	TElnet
25	TCP	SMTP (simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol version 3)
119	TCP	NEWS (Network News Transfer Protocol)
123	UDP	NTP (Network Time Protocol)
161	TCP	SNMP
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
4000	TCP	ICQ
7070	UDP	Real Audio

Port Mapping



Application: Select the service you wish to configure.

Protocol: A protocol is automatically applied when an Application is selected from the listbox or you may select a protocol type which you want.

External Port & Internal Port: Enter the public port number & range you wish to configure.

Internal IP Address: Enter the IP address of a specific internal server to which requests from the specified port is forwarded.

Add: Click to add a new virtual server rule. Click again and the next figure appears.

Edit: Check the Edit radio button to display the parameter of the selected application, then after changing the parameters click the Edit/Delete button to apply the changes.

Delete: To remove a port mapping application, check the Remove box of the selected application then click the Edit/Delete button.

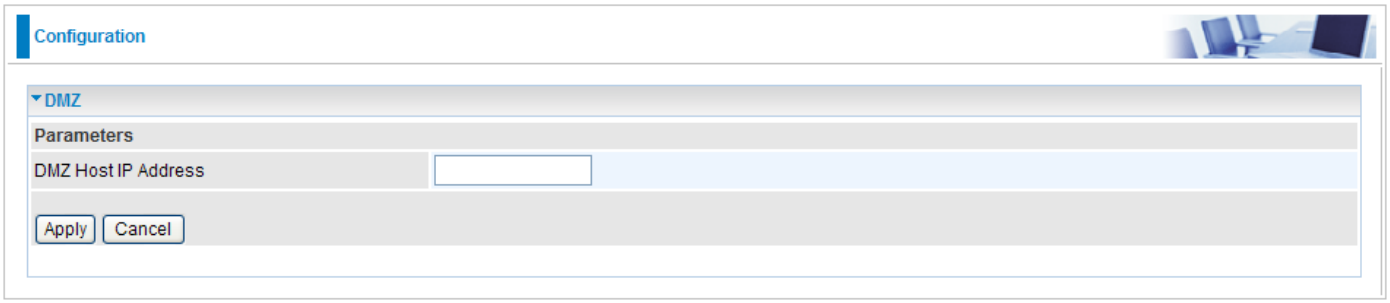
Since NAT acts as a “natural” Internet firewall, your router protects your network from accessed by outside users, as all incoming connection attempts point to your router unless you specifically create Virtual Server entries to forward those ports to a PC on your network. When your router needs to allow outside users to access internal servers, e.g. a web server, FTP server, Email server or game server, the router can act as a “virtual server”. You can set up a local server with a specific port number for the service to use, e.g. web/HTTP (port 80), FTP (port 21), Telnet (port 23), SMTP (port 25), or POP3 (port 110). When an incoming access request the router for a specified port is received, it is forwarded to the corresponding internal server.

For example, if you set the port number 80 (Web/HTTP) to be mapped to the IP Address 192.168.1.2, then all incoming HTTP requests from outside users are forwarded to the local server (PC) with the IP address of 192.168.1.2. If the port is not listed as a predefined application, you need to add it manually.

In addition to specifying the port number used, you also need to specify the protocol used. The protocol is determined by a particular application. Most applications use TCP or UDP, however you may also specify other protocols using the drop-down Protocol menu. Setting the protocol to “all” causes all incoming connection attempts using all protocols on all port numbers to be forwarded to the specified IP address.

DMZ

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets that do not use a port number which is already used by any other Virtual Server entries will first be checked by the Firewall and NAT algorithms before it is passed to the DMZ host.



Attention

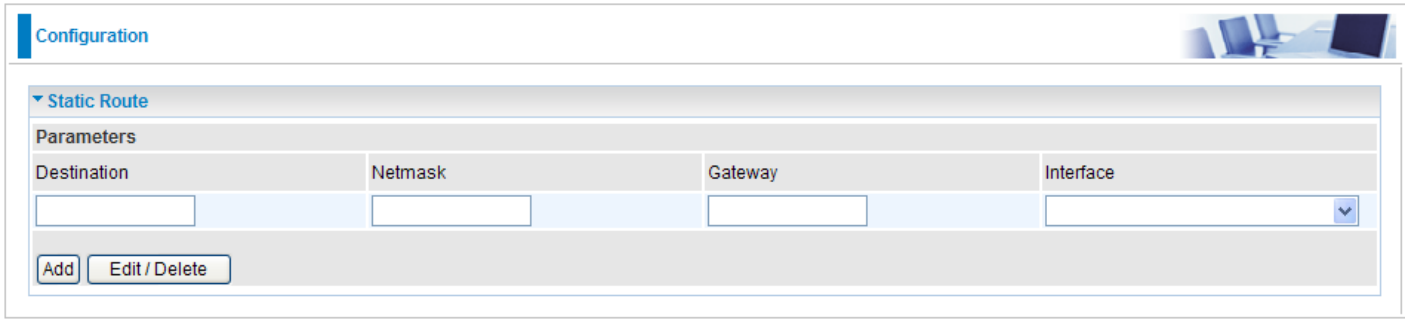
If you have disabled the NAT option in the WAN-ISP section, the Virtual Server will hence become invalid. If the DHCP option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.

NOTE:

Since outside users are able to connect to the PCs on your network, port mapping utilization imposes security implications. You are therefore adviced to use specific Virtual Server entries just for those ports that your applications require.

Advanced

Static Route

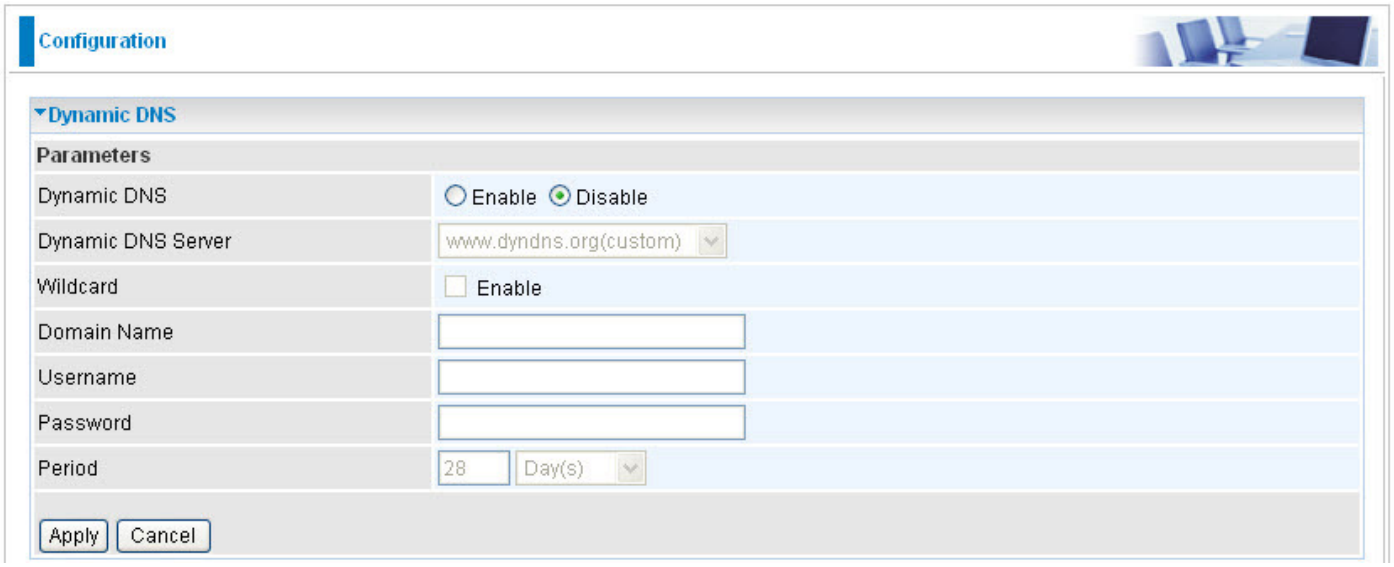


Enter the destination network address, subnet mask, gateway AND/OR the available WAN interface, then click “Add” to add a new entry to the routing table.

Dynamic DNS

The Dynamic DNS function lets you alias a dynamic IP address to a static hostname, so if your ISP does not assign you a static IP address you can still use a domain name. This is especially useful when hosting servers via your ADSL connection, so that anyone wishing to connect to you may use your domain name, rather than the dynamic IP address which is assigned to you by ISP.

You need to first register and establish an account with the Dynamic DNS provider using their website, for example **http://www.dyndns.org/**



Dynamic DNS Server: Select the DDNS service you have registered an account with.

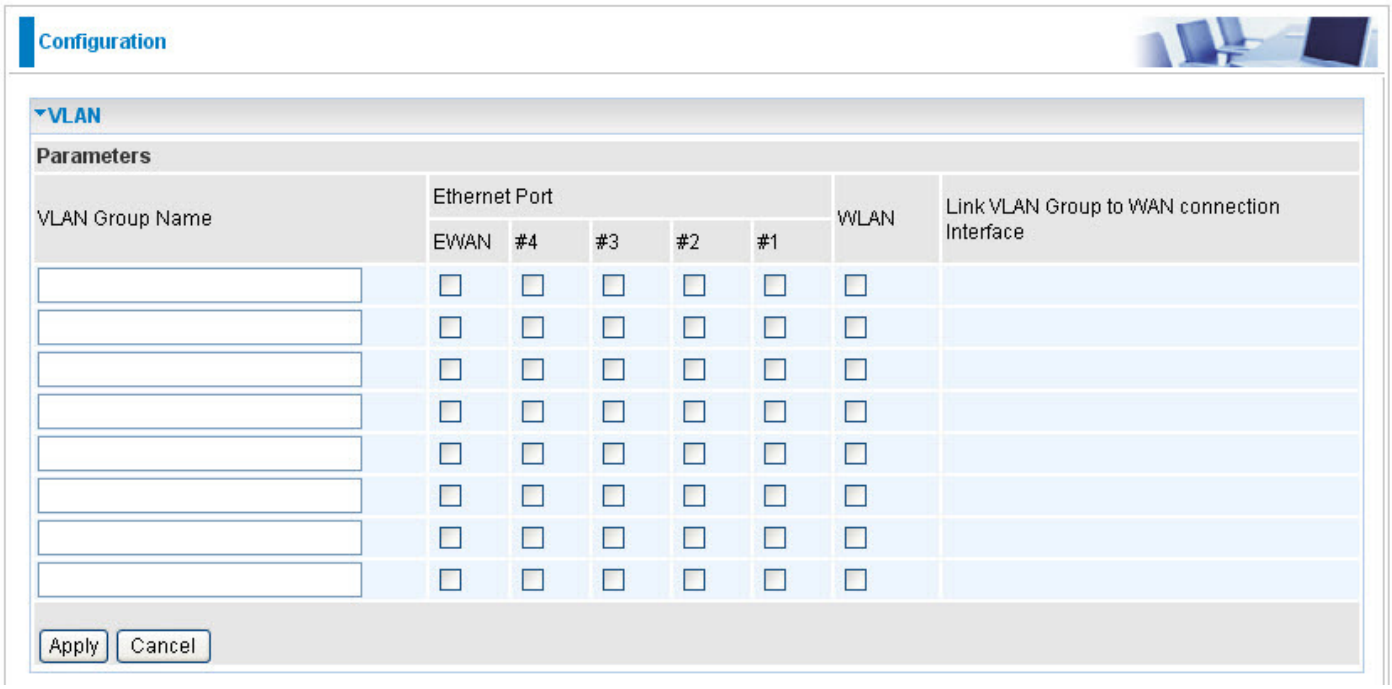
Wildcard: When enabled, you allow the system to lookup on domain names that do not exist to have MX records synthesized for them.

Domain Name, Username and Password: Enter your registered domain name and your username and password for this service.

Period: Enter the length of the period in the blank, you can set the period unit in day (d), hour (H) or month (M).

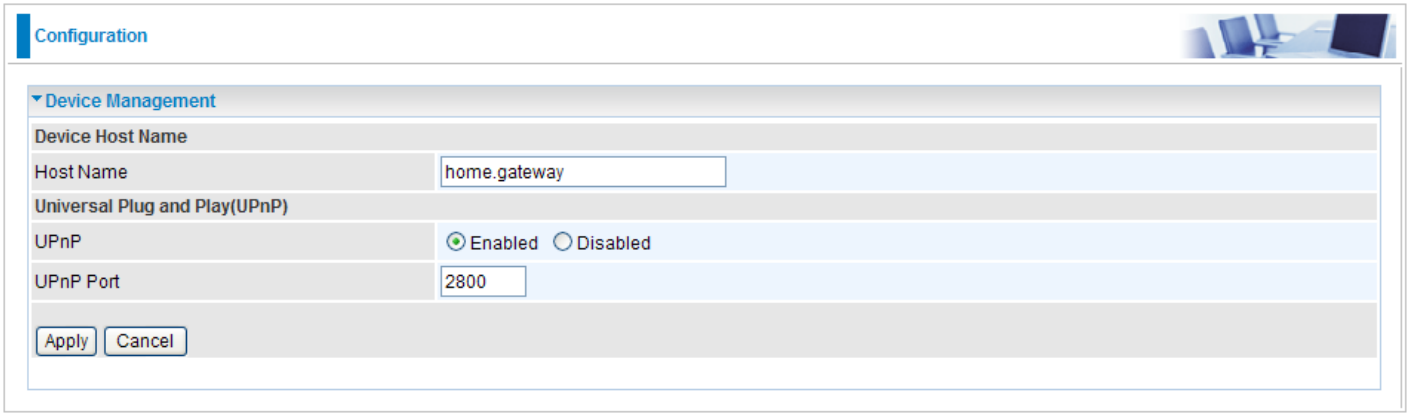
VLAN

VLAN (Virtual Local Area Network) is a group of devices on different physical LAN segments that can communicate with each other as if they were all on the same physical LAN segment.



Device Management

The Device Management advanced configuration settings allow you to control your router's security options and device monitoring features.



UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with the feature to control data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems. By letting the application control the required settings and removing the need for the user to control the advanced configuration of their device will make tasks such as port forwarding become easier.

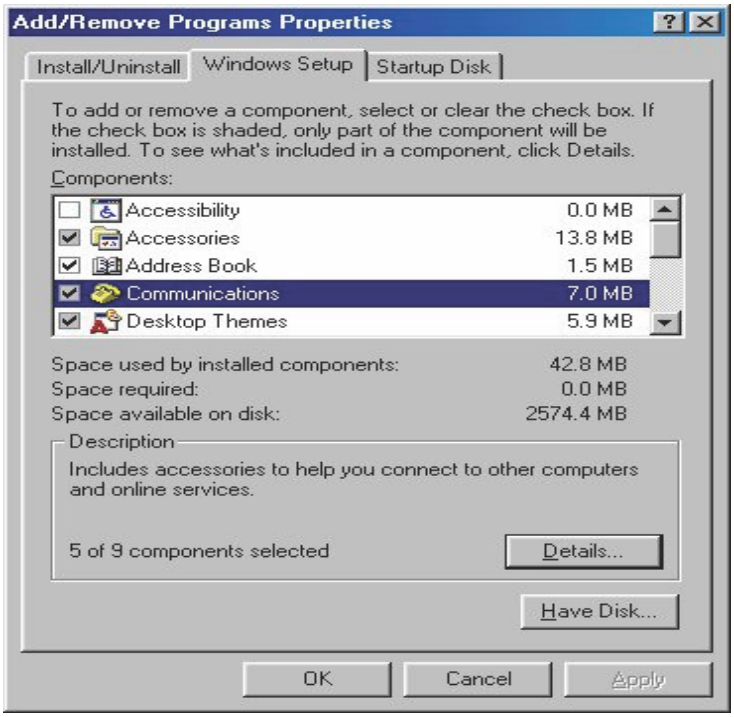
Both user's Operating System and its relevant applications must support UPnP in addition to the router. Windows XP and Windows Me have a native built-in support for UPnP (when the component is installed). Windows 98 users may have to install the Internet Connection Sharing client from Windows XP in order to support UpnP feature. Windows 2000 does not support UPnP.

Installing UPnP in Windows Example

Follow the steps below to install the UPnP in Windows Me.

Step 1: Click Start and Control Panel. Double-click Add/Remove Programs.

Step 2: Click on the Windows Setup tab and select Communication in the Components selection box. Click Details.


Add/Remove Programs Properties
Install/Uninstall
Windows Setup
Startup Disk
To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.
Components:
Accessibility 0.0 MB
Accessories 13.8 MB
Address Book 1.5 MB
Communications 7.0 MB
Desktop Themes 5.9 MB
Space used by installed components: 42.8 MB
Space required: 0.0 MB
Space available on disk: 2574.4 MB
Description
Includes accessories to help you connect to other computers and online services.
5 of 9 components selected
Details...
Have Disk...
OK
Cancel
Apply

Step 3: In the Communications window, select the Universal Plug and Play check box in the Components selection box.

Communications
To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
NetMeeting 4.2 MB
Phone Dialer 0.2 MB
Universal Plug and Play 0.4 MB
Virtual Private Networking 0.0 MB
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB
Description
Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.
Details...
OK
Cancel

Step 4: Click OK to go back to the Add/Remove Programs Properties window. Click Next.

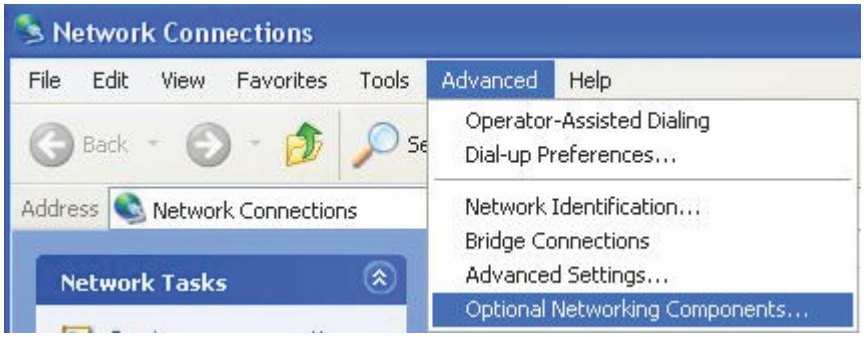
Step 5: Restart the computer when prompted.

Follow the steps below to install the UPnP in Windows XP.

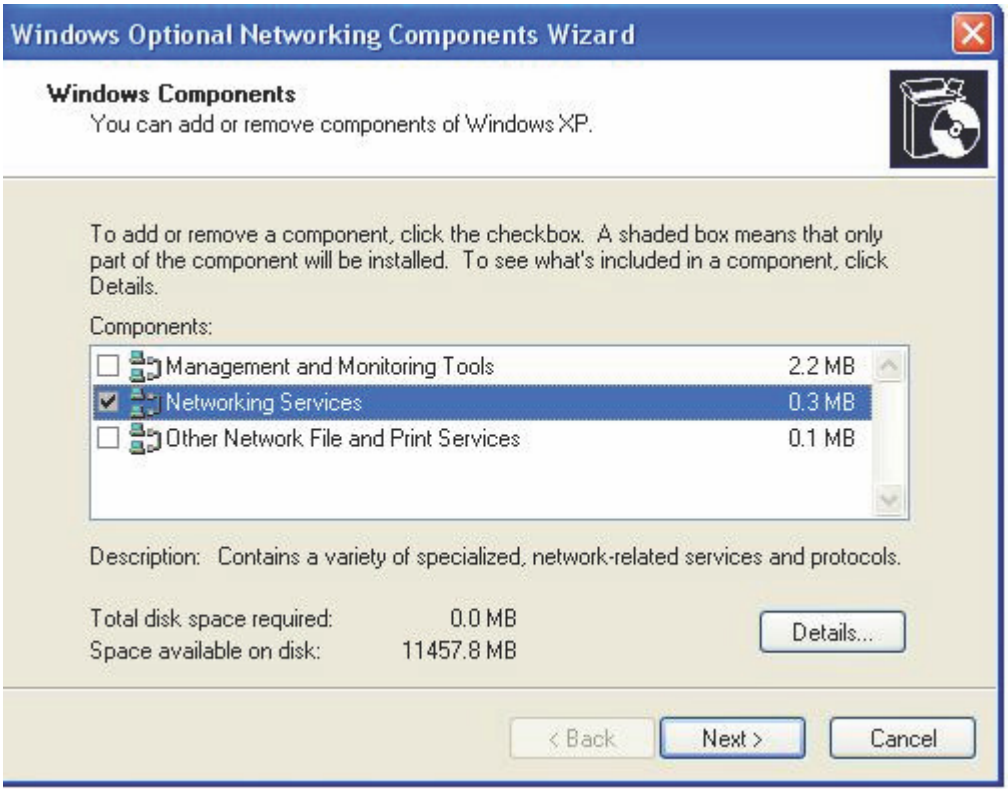
Step 1: Click Start and Control Panel.

Step 2: Double-click Network Connections.

Step 3: In the Network Connections window, click Advanced in the main menu and select Optional Networking Components ….

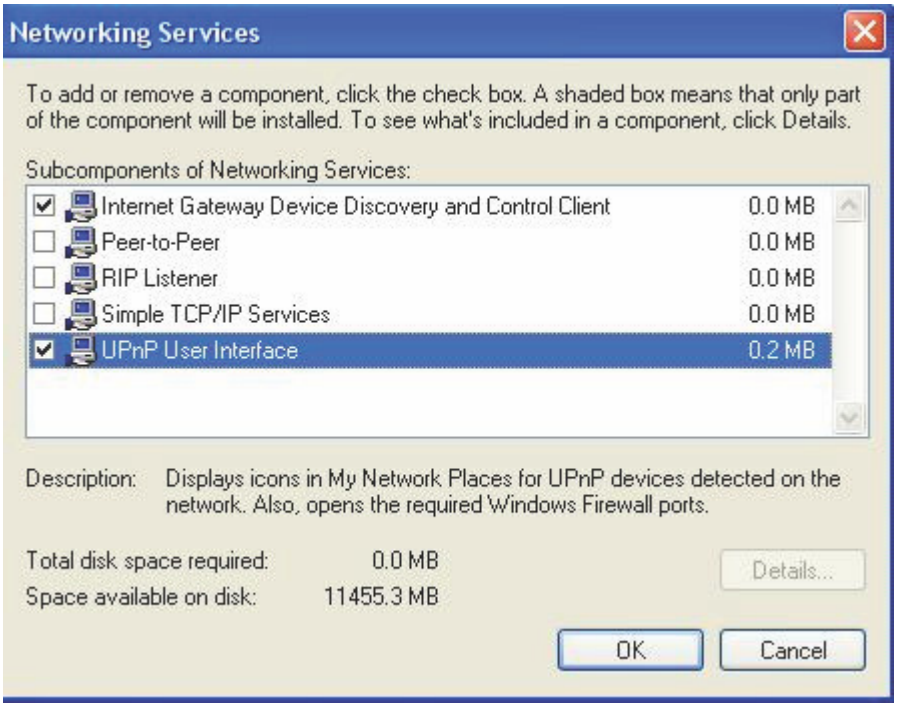


Step 4: When the Windows Optional Networking Components Wizard window appears, select Networking Service in the Components selection box and click Details.


Windows Optional Networking Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Management and Monitoring Tools 2.2 MB
Networking Services 0.3 MB
Other Network File and Print Services 0.1 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 0.0 MB
Space available on disk: 11457.8 MB
Details...
< Back
Next >
Cancel

Step 5: In the Networking Services window, select the Universal Plug and Play check box.

Step 6: Click OK to go back to the Windows Optional Networking Component Wizard window and click Next.


Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
Internet Gateway Device Discovery and Control Client 0.0 MB
Peer-to-Peer 0.0 MB
RIP Listener 0.0 MB
Simple TCP/IP Services 0.0 MB
UPnP User Interface 0.2 MB
Description: Displays icons in My Network Places for UPnP devices detected on the network. Also, opens the required Windows Firewall ports.
Total disk space required: 0.0 MB
Space available on disk: 11455.3 MB
Details...
OK
Cancel

Auto-discover Your UPnP-enabled Network Device

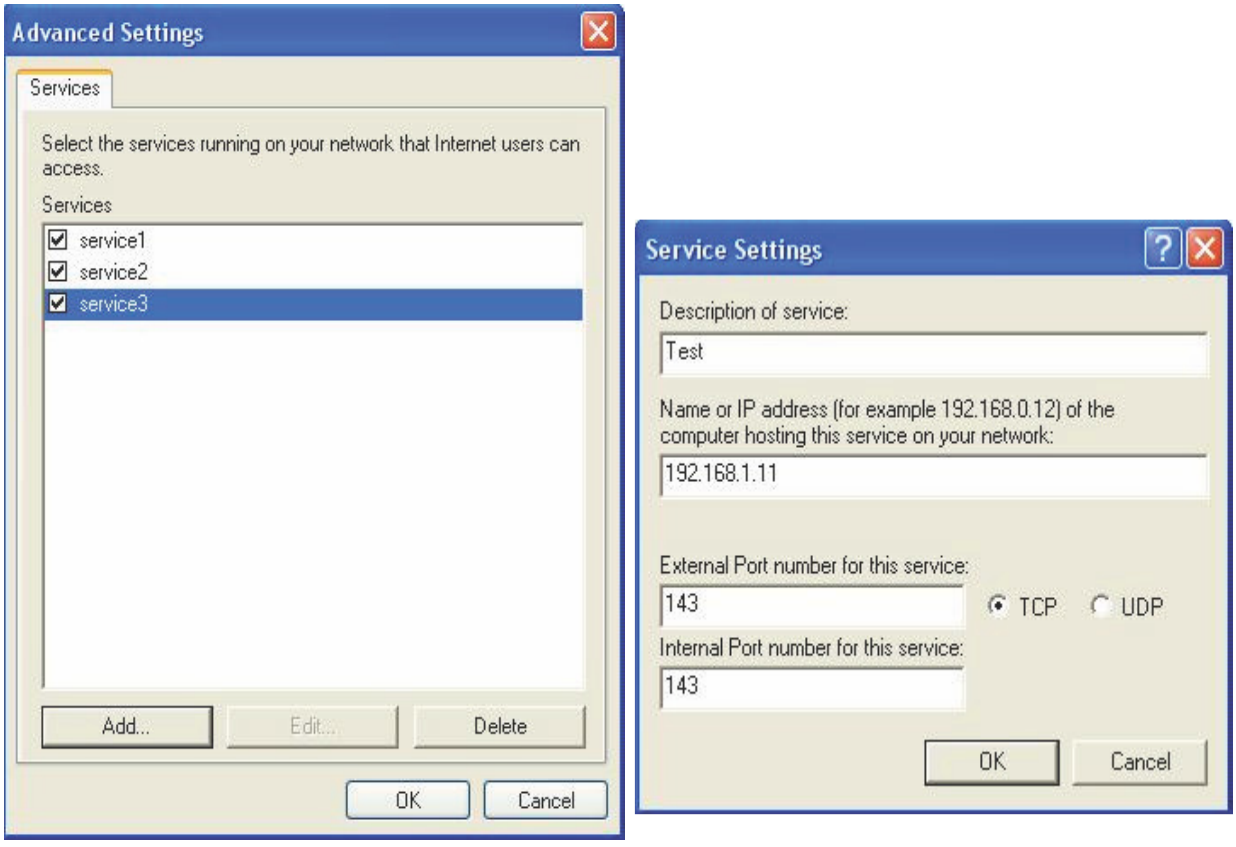
Step 1: Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.

Step 2: Right-click the icon and select Properties.

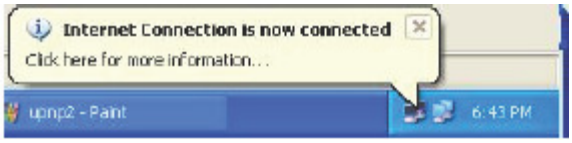
Step 3: In the Internet Connection Properties window, click Settings to see the port mappings that were automatically created.

Internet Connection Properties
General
Connect to the Internet using:
Internet Connection
This connection allows you to connect to the Internet through a shared connection on another computer.
Settings...
Show icon in notification area when connected
OK
Cancel

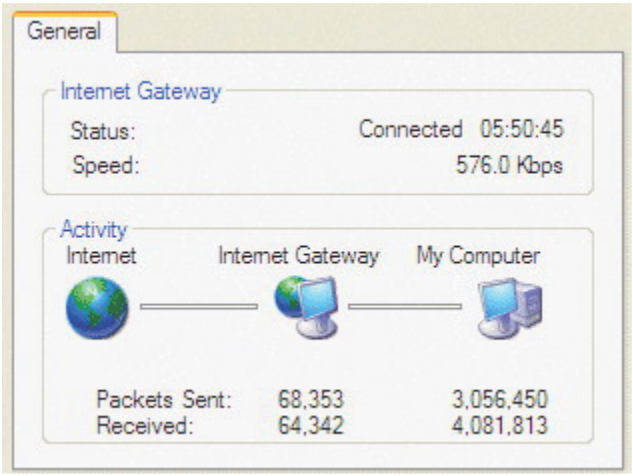
Step 4: You may edit or delete the port mappings or click Add to manually add port mappings.



Step 5: Select Show icon in notification area when connected option and click OK. An icon displays in the system tray.



Step 6: Double-click on the icon to display your current Internet connection status.



Web Configurator Easy Access

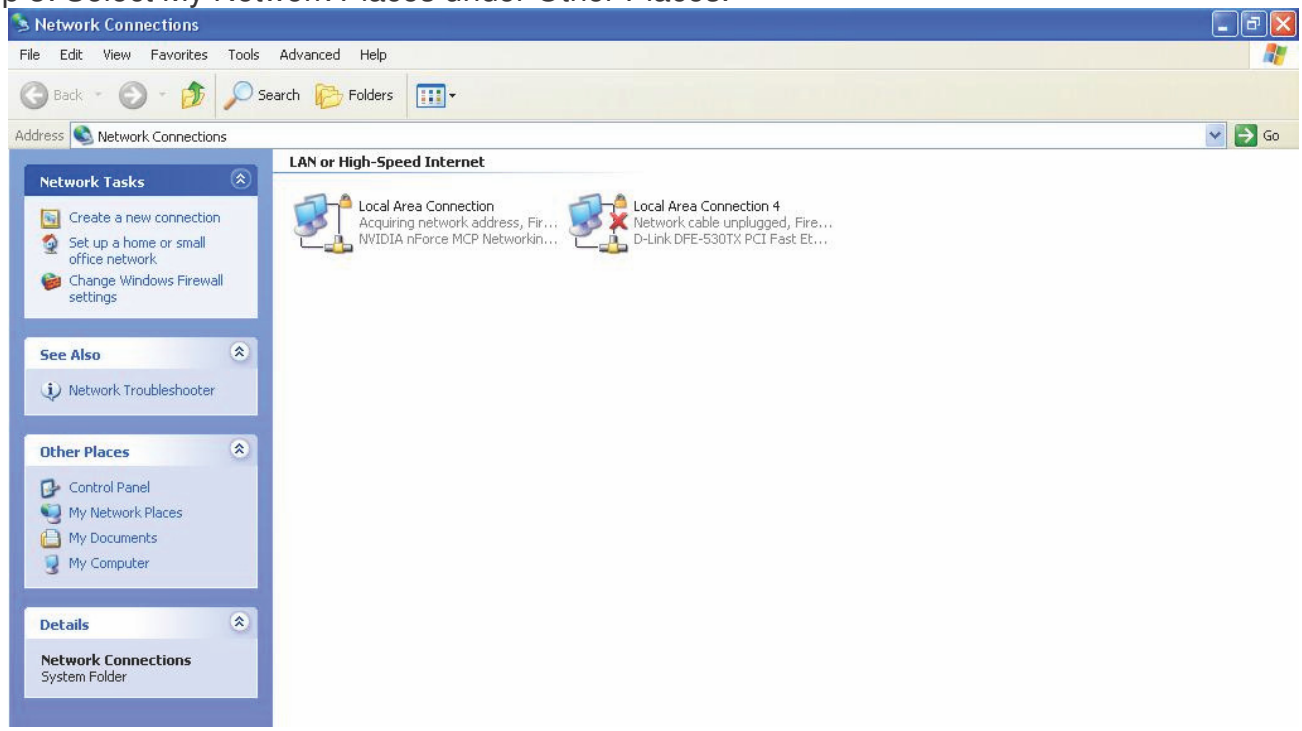
With UPnP, you can access web-based configuration for the BEC 7800 without first finding out the IP address of the router. This helps if you do not know the router's IP address.

Follow the steps below to access web configuration.

Step 1: Click Start and then Control Panel.

Step 2: Double-click Network Connections.

Step 3: Select My Network Places under Other Places.

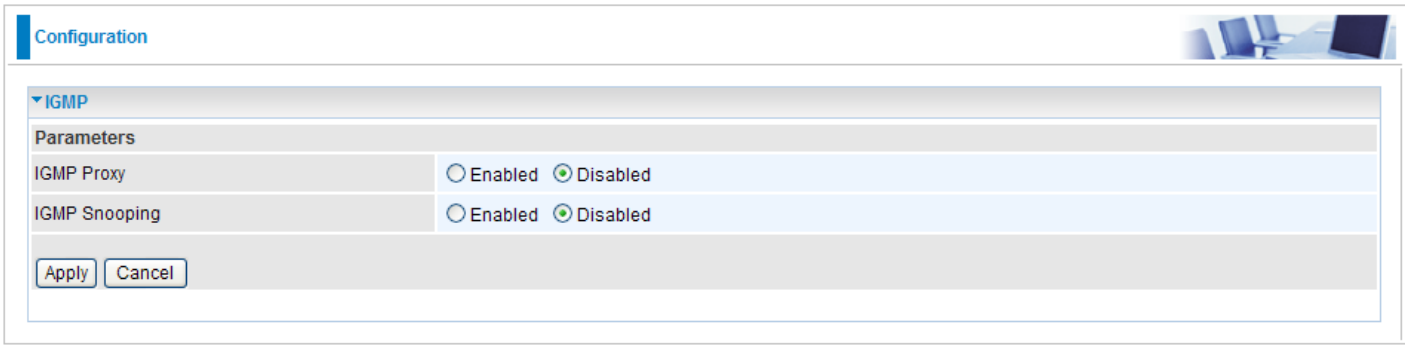


Step 4: An icon describing each UPnP-enabled device shows under Local Network.

Step 5: Right-click on the icon of your BEC 7800 and select Invoke. The web configuration login screen displays.

Step 6: Right-click on the icon of your BEC 7800 and select Properties. A properties window displays basic information about the BEC 7800.

IGMP



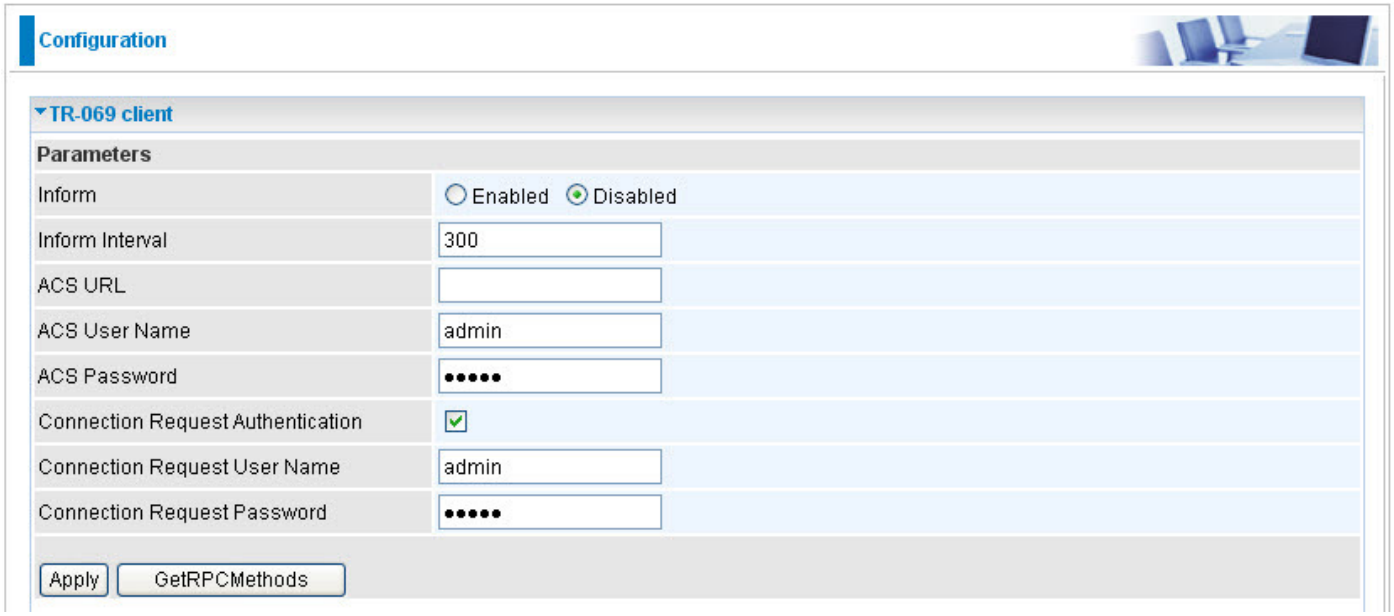
IGMP, known as Internet Group Management Protocol, is used to manage hosts from multicast group.

IGMP Proxy: Accepting multicast packet. Default is set to Disable.

IGMP Snooping: Allowing switched Ethernet / Wireless to check and make correct forwarding decisions. Default is set to Disable.

TR-069 Client

Please contact you ISP for the information of TR069.



Inform: You may enable or disable the periodic inform feature.

Inform Interval: Enter the length of the periodic inform interval (unit: seconds).

ACS URL: Enter the ACS URL address.

ACS User Name: Enter the ACS server login name.

ACS Password: Enter the ACS server login password.

Connection Request Authentication: Check off to enable connection request authentication feature.

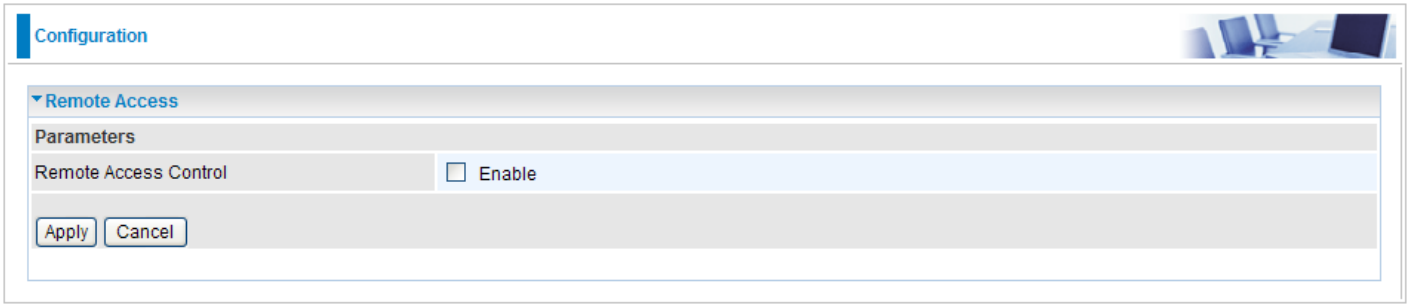
Connection Request User Name: Enter the username for ACS server to make connection request.

Connection Request Password: Enter the password for ACS server to make connection request.

GetRPCMethod: Detect the types of methods that ACS supports and is in communication with.

Remote Access

Remote Access Control: Select Enable to allow management access from remote side (mostly from internet).



Appendix: Product Support & Contact

If you come across any problems please contact the dealer from where you purchased your product.

Contact BEC

Worldwide:

http://www.bectechnologies.com

MAC OS is a registered Trademark of Apple Computer, Inc.

Windows 98, Windows NT, Windows 2000, Windows Me, Windows XP and Windows Vista are registered Trademarks of Microsoft Corporation.